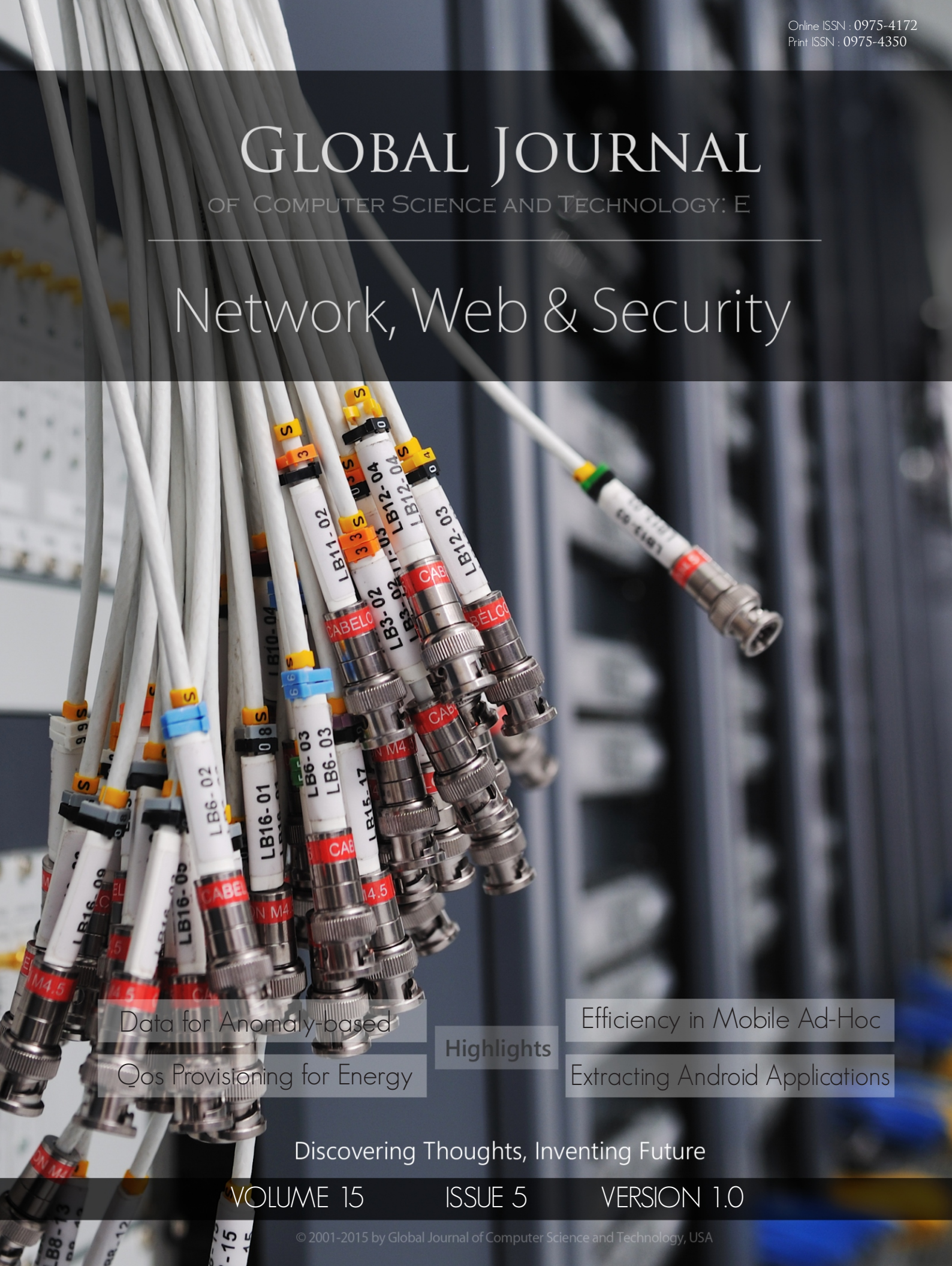
Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Highlights

Data for Anomaly-based Qos Provisioning for Energy

Efficiency in Mobile Ad-Hoc Extracting Android Applications

Discovering Thoughts, Inventing Future

VOLUME 15 ISSUE 5 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 15 Issue 5 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board
(Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo,School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, TaiwanUniversity Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Contents of the Issue

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Extracting Android Applications Data for Anomaly-based Malware Detection

By Joshua Abah, Waziri O.V., Abdullahi M.B., Ume U.A. & Adewale O.S.
University of Technology Minna, Nigeria

Abstract- In order to apply any machine learning algorithm or classifier, it is fundamentally important to first and foremost collect relevant features. This is most important in the field of dynamic analysis approach to anomaly malware detection systems. In this approach, the behaviour patterns of applications while in execution are analysed. The behaviour features that Android as a system allows access permissions to depend on the type of device; either rooted or not. Android is based on the Linux kernel at the bottom layer, all layers on top of the kernel run without privileged mode. Thus, if a behaviour feature vector is created from features of Android (Application Programming Interface) API in unrooted mode, then only system information made available by Android can be used. In this paper, a Device Monitoring system for an unrooted device is developed and used to collect Android application data. The application data is used to build feature vectors that describes the Android application behaviour for Anomaly malware detection.

Keywords: *android, anomaly detection, application behaviours, feature vectors, malware detection, mobile device, rooted, unrooted.*

GJCST-E Classification : *C.1.3 D.4.6*

Strictly as per the compliance and regulations of:

Extracting Android Applications Data for Anomaly-based Malware Detection

Joshua Abah [α], Waziri O.V. [σ], Abdullahi M.B. [ρ], Ume U.A. [ω] & Adewale O.S. [¥]

Abstract- In order to apply any machine learning algorithm or classifier, it is fundamentally important to first and foremost collect relevant features. This is most important in the field of dynamic analysis approach to anomaly malware detection systems. In this approach, the behaviour patterns of applications while in execution are analysed. The behaviour features that Android as a system allows access permissions to depend on the type of device; either rooted or not. Android is based on the Linux kernel at the bottom layer, all layers on top of the kernel run without privileged mode. Thus, if a behaviour feature vector is created from features of Android (Application Programming Interface) API in unrooted mode, then only system information made available by Android can be used. In this paper, a Device Monitoring system for an unrooted device is developed and used to collect Android application data. The application data is used to build feature vectors that describes the Android application behaviour for Anomaly malware detection. This application is able to collect essential information from Android application such as installed applications and services running within the device before or after the Monitoring application was started, the date/time stamp, calls initiated from the device, calls received by the device, sent short message services (SMSs), SMSs received, and the status of the device as at when the event took place. This information is logged in a comma separated value (.csv) file format and stored on the SDcard of the device. The .csv file is converted to attribute relation file format (.arff); the format acceptable by WEKA machine learning tool. This. arff file of feature vectors is then used as input to the Classifier in the Android malware detection system.

Keywords: android, anomaly detection, application behaviours, feature vectors, malware detection, mobile device, rooted, unrooted.

I. Introduction

Android is one of the most used Smartphone's operating System in the World (Srikanth, 2012). Android is open source with huge user community and documentations as a result of these, it allows any programmer to develop and publish Applications to both the Official or Unofficial market. There are over seven hundred thousand Applications published via the Official Android market, the Google Play Store (Zack, 2012). Malware attack is a challenging issue among the Android user community. This is due to its open source and a very huge adoption and market penetration, making it a target for most malware developers. Android is predicted to be the most used mobile Smartphone platform by 2014 (You, Daeyeol, Hyung-Woo, Jae &Jeong,2014) which has become a reality. This ubiquitous gains of Android brings along with it security risks in terms of malware attacks targeted at this platform. It therefore becomes necessary to make the platform safe for users by providing defence mechanism especially against malware.

There are basically three approaches according to (Burquera, Zurutuza&Nadjm-Tehrani,2011);(Aswathy, 2013); (Lovi&Divya, 2014) to mobile malware detection approaches; static, dynamic and manifest file analyses. While Static analysis focused on the use of patterns of strings called signatures to detect malware presence, dynamic analysis approach to malware detection uses the behaviour pattern of Applications while in execution. The third approach involves the analysis of Android Manifest file. This paper presents a model for mining Applications behaviours for detecting malware on the Android platform using dynamic analysis.

The malware detector attempts to help protect the system by detecting malicious behaviour (Aswathy, 2013). The malware detector performs its protection through the manifested malware detection Approaches.Detection methods for attacks on mobile devices (Burquera, Zurutuza&Nadjm-Tehrani2011);(Wei, Mao, Jeng, Lee, Wang& Wu, 2012); (Wu, Mao, Wei, Lee & Wu, 2012);(Ham, Choi, Lee, Lim & Kim, 2012) have been proposed to reduce the damage from the distribution of malicious applications. However, a mechanism that provides more accurate ways of determining normal applications and malicious applications on Android mobile devices must be developed and a procedure for obtaining the features well defined. This paper developed a model for extracting Android application behaviours through events of normal applications and malicious applications, using a customized approach.

The research employs Anomaly-based detection in a host-based manner to monitor activity that occurs on the target host system. This system is capable of monitoring features of the Android system such as calls received, calls initiated, system calls invoked by running applications, Short Messaging

Author α ρ ¥ : Department of Computer Science, Federal University of Technology Minna, Nigeria. e-mails: jehoshua_a@yahoo.com, abah@unimaid.edu.ng, el.bashir02@futminna.edu.ng, adewale@futa.edu.ng

Author σ : Department of Cyber Security Science, Federal University of Technology Minna, Nigeria. e-mail: victor.waziri@futminna.edu.ng, onomzavictor@gmail.com

Author ω : Department of Information and Media Technology, Federal University of Technology Minna, Nigeria. e-mail: drarthurume@gmail.com

Services (SMSs) received, SMSs sent and screen status of the target device. Anomaly-based detection systems use a prior training phase to establish a normality model for the system activity. In this method of detection, the detection system is first trained on the normal behaviour of the application or target system to be monitored. Using this normality model of behaviour, it becomes possible to detect anomalous activities by looking for abnormal behaviour or activities that deviate from the defined normal behaviour occurring in the system. Though this technique look more complex, it has the advantage of being able to detect new and unknown malware attacks. Anomaly-based detection requires the use of feature vectors to train the classifier before subsequent classification can be carried out. These feature vectors are obtained from features or data collected from the system.

The objective of this work is to extract Android applications data from an unrooted android device and using them to effectively describe the system behaviour. The structure of this paper is given as follows: section one provides a brief introduction; section two gives related literatures; section three discuss the Experimental procedures and setup; section four provides the discussion of result; section five provide the hardware and software used for the experimentation and finally, section six gives the summary and conclusion of the work.

II. Related Works

Android malware detection systems available currently employs static approach to malware detection by scanning files for byte sequences of known malware Applications. Anomaly-based detection is still in a developmental stage and researches are ongoing. As a result, the current approaches are not able to detect unknown attacks. Unknown malware attacks also referred to as 'zero day attacks' are attacks carried out by unknown malware whose signatures have not been analysed and obtained. Several approaches with different metrics for defining Android application behaviours have been developed and are discussed.

You Jounget *al*. (2014);You Joung&Hyung-Woo, (2014)presented an approach for determining malicious attack on Android using System Call Event Pattern Analysis. In their work, system calls invoked by executing Applications of different categories and their frequency of occurrences is used as the metrics for defining Applications behaviour. Their analysis was carried out on Linux system rather than on mobile device. Abelaet *al.*(2013) developed AMDA an automated malware detection system for the Android platform. The core modules of the system included the Feature Extraction Module and the Behaviour Analysis Module. The Feature Extraction Module generates activity log from running applications retrieved from the application repository of the system. The activity log contains the system calls from application activity which are the features that the module retrieves.

Mohammed *et al.* (2014) in the Automatic Feature Extraction part of their work proposed and implemented an approach to detect malicious applications statically through a set of well-defined APIs. Similarly, Tchakounté, &Dayang (2013) used a static approach to analyse System calls of malware on the Android platform.Lin *et al*, (2013)proposed SCSdroid, which uses the thread-grained system calls sequences, because these sequences can be regarded as the actual behaviour of the application. Their approach is a step further from just system calls of Applications to carter for malware repackaged applications. Luoxu & Qinghua, (2013) presented a static approach to their Runtime-based Behaviour Dynamic Analysis System for Android Malware Detection. They used Loadable Kernel Module hooking to hook the Android system and then collect *data.* The collected data consist of IMSI, SIM, IMEI, TEL, call log, SMS, MAIL and so on. The technology of analysis is semantic analysis and regular expression.

Yousra, Wenliang&Heng,(2013) used APIs as the feature for describing Android behaviours used for detecting malware. To select the best features that distinguish between malware from benign applications, API level information within the bytecode were used since it conveys substantial semantics about the apps behaviour. More specifically, they focused on critical API calls, their package level information, as well as their parameters. Dini, Martinelli, Saracino&Sgandurra, (2012)employed two-layer applications behaviour features in order to properly described Android malware behaviours. These include System calls from the kernel layer and other features from the Applications layer. This approach tend to provide a better description of the system than a monolithic view of just a single layer as it considered both the Operating System layer behaviours and the Applications layer behaviours.

It is observed from all the reviewed literatures that System calls pattern analysis played a critical role in providing Android Applications behaviour pattern. It is therefore clear that System calls as features could best be used either singly or in addition to other features to describe Application behaviours not just in Android but any mobile platform.

III. Experimental Procedures and Setup

In this section, the various activities carried out and the different modules implemented to ensure application feature behaviours are intercepted for use in malware detection process are discussed. But before then we show the big picture of the entire malware detection system in a schematic form as in Figure 1.0.

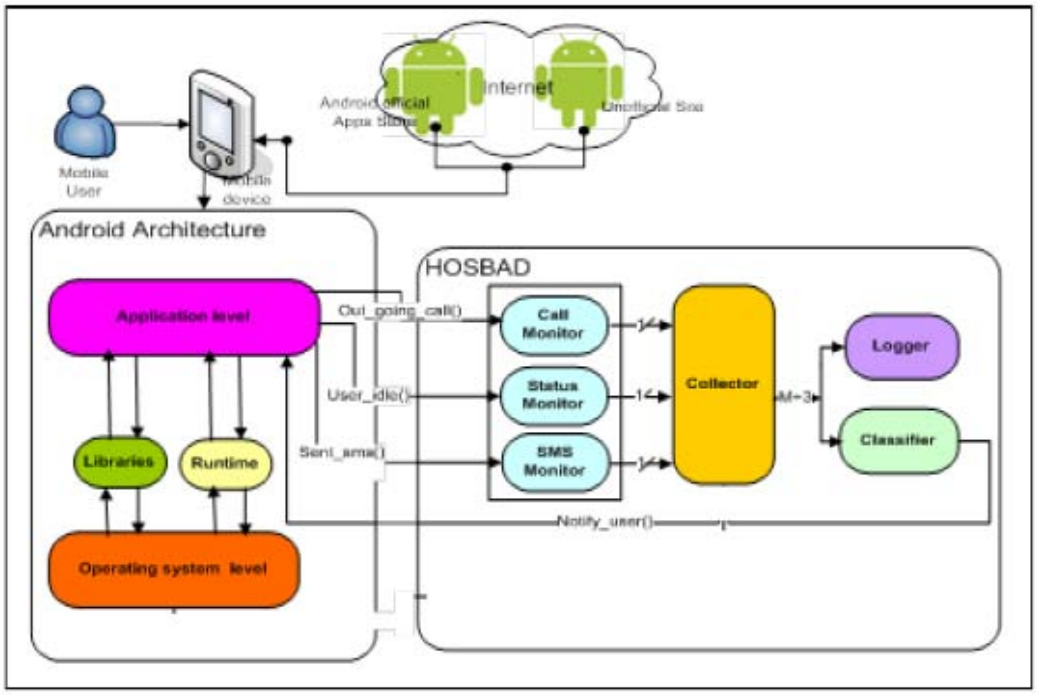


Figure 1. 0 : Architecture of the Android Malware Detection System (HOSBAD)

a) Application Acquisition Process

The Application Acquisition process involves downloading applications from Android Markets and storing them into the application repository folder. Applications which could be normal or malicious are downloaded both from the Official Android market and unofficial Android markets. Figure 1.1 shows the Application acquisition processes.

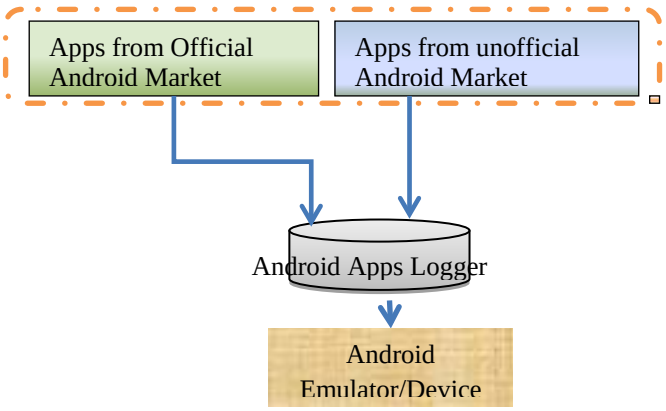


Figure 1. 1: Schematic of Application Acquisition Process

Each of these Applications is executed in an instrumented Android emulator via Android Virtual Device (AVD). An Android 2.3.3 software development kit (SDK) emulator is used to run the Android applications because this is the only medium to automate the generation of application system activity logs without using an actual mobile device. There is no much actual difference to using human input to be able to activate the behavioural activity of an application. However, the log data contains activities which are irrelevant for detection of malicious activity. With this problem of noise in the log data, the system utilizes a self-developed parser which is customized as to which features are to be collected.

b) The Data Collection Processes

In order to collect the Android Applications data, the various monitors described are implemented as Android java programs in the Device Monitoring Application. This application is actually just a module in the complete detection system called HOSBAD. The application will serve as the feature mining model which will run on the Android device to collect the features while the user interacts with Applications on the device. The feature mining model will monitor Android application activities implemented using a broadcast receiver and record on going activity taking place on the device. Figure 1.2 shows the data collection stages by the feature mining model.

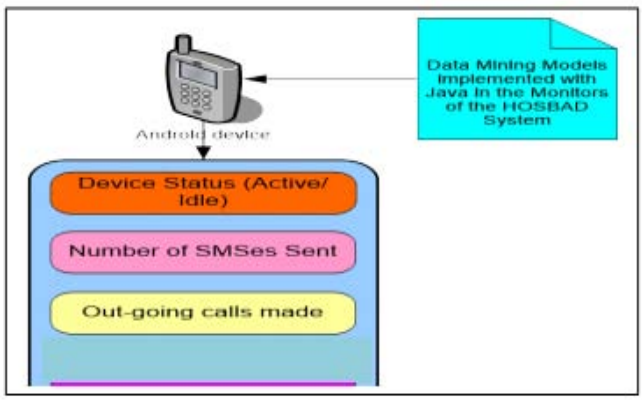


Figure 1. 2 : The Data Collection Process

The *collector* module in conjunction with the monitors will help to collect as much information as possible from the Android Applications installed on the device. This information include the Date/Time stamp, the application and services running on the device, out-going calls, incoming calls, out-going SMS, incoming SMS, and Device screen status. This information is collectively referred to as feature of application or behaviours . For each .apk file, the device user interaction is created or the emulator simulates user interaction by randomly interacting with the application interface. It should be note that due to the numerous Android Applications available in the Android market, it is not possible for one to monitor and record all Applications for the numerous available Android Applications, doing this will require the researcher to spend many years collecting all of the information about Applications available in the Android market. For this reason, few of the Applications were selected.

c) Android Feature Collection

In order to apply any machine learning algorithm or classifier, it is fundamentally important to first and foremost collect relevant features. The features that Android as a system allows access permissions to depend on the type of device. The type of device here implies whether the device has been rooted or not. Android is based on the Linux kernel at the bottom layer, all layers on top of the kernel layer run without privileged mode. That is, all applications and system libraries are inside a virtual application sandbox. As a result of this architecture, applications are prohibited from accessing other application data (unless explicitly granted permission by other applications called the rooting applications). Thus, if a feature vector is created from features of Android API in unrooted mode, then only system information made available by Android can be used. On the other hand, having a rooted device allows one to install system tools that could gather features from underlying host and network behaviour but doing this subject the device to serious security vulnerabilities as the entire device file system will be opened up to attacks.

In this Work, an unrooted device is used in order to collect Android application data. To be able to do this, a feature mining model which is a self-developed application module that will be part of the detection system is used. This application is able to collect essential information from Android application such as installed applications and services running within the device before or after the Monitoring application was started, the date/time stamp, calls initiated from the device (outCalls), calls received by the device (InCalls), sent SMSs (OutSMS), SMSs received (InSMS), and the status of the device (Screen) as at when the event took place. This information is written into a log file and stored on the SDcard of the device. This log file is a comma separated value in .csv format. Parsing these data with another self-developed code module will produce the feature vectors which is in .arff file format; the format acceptable by WEKA. This self-developed code module that serves as a feature mining model for application enable us to create a folder were all monitored/recorded application logs in csv file format will be stored. This csv file will be parsed by another parserto make feature vector file in arff. This arff file of feature vectors will be used as input to the Classifier in the Android malware detection system.

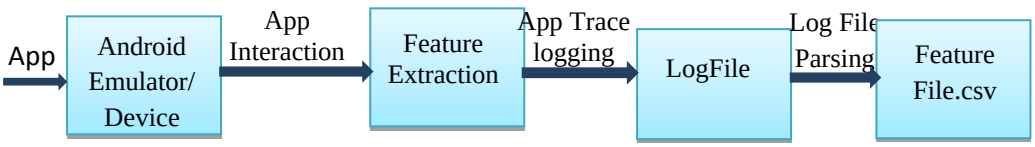


Figure 1. 3 : Features Extraction Processes

The data extraction application performs the following major task as it runs either in foreground or background. This is represented in Figure 1.3: the features extraction processes.

i. First, the Android application runs either on the emulator or real device, the Device Monitoring which implements the feature extraction model; a self-developed module that implements the monitors runs in the background to intercepts and records the specified features (out call, in call, out SMS, in SMS, and device status).

ii. Secondly, the log stream is input to the parser in the Device Monitoring application and is parsed by filtering and formatting the log data to a readable form in a comma separated value (csv) format.

iii. Finally, the csv file will then be parsed by another parser to generate a .arff file that will be used by the classifier.

i. *Implementation Details*

Although the code for the Device Monitoring application which is the data extraction model cannot be given here, the skeletal description of the different modules representing the respective monitors is presented. The broadcast receiver class for the calls and receiving incoming SMS record the calls and SMS events into app preferences, there is no proper receiver for the outgoing SMS so special observer class is used in the service class. When this receiver is started in service, it doesn't work on real device, so it is registered

in the manifest and the preferences is used. The structure of the public class; ReceiverCallSms that implements the calls and the SMS is given as;

```
public class  ReceiverCallSms extends
BroadcastReceiver {
```

Within this class, the methods for the calls (out-going and in-coming calls) and the in-coming SMS are implemented in a single method with a nexted*if ..else* statement.

The Inner broadcast receiver for monitoring the screen condition is implemented with the class ScreenReceiver which implements the onReceive method using special observer "intent".

The service monitoring is implemented by a class Service Monitoring with a method that records the services running on the device and the features to be extracted. The Binder function initiates the monitoring process when the start button is clicked and to stop the monitoring when the stop button is clicked. All monitored events and activities are written to a file in a comma separated value format. The method checks for the presence of an SD card and create a folder there where the file will be stored or setup a Gmail account where the file will be sent to without user interference. The file is named using the device date/time stamp.csv.

```
07.10.2015 20:33:55,Monitoring Started
Time,AppName,OutCall,InCall,OutSMS,InSMS,Screen,Class
 before,YouTube,0,0,0,0,1,?
 before,Launcher,0,0,0,0,1,?
 before,Torch,0,0,0,0,1,?
 before,Opera Mini beta,0,0,0,0,1,?
 before,Contacts,0,0,0,0,1,?
 before,Phone,0,0,0,0,1,?
```

Figure 1.4 shows a screenshot of the feature mining model application for the malware detection system.

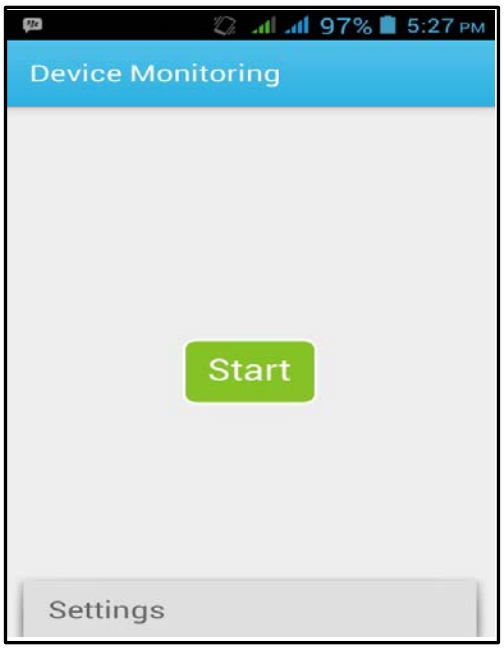


Figure 1.4 : Feature Mining Model Application

The settings menu provides the avenue for creating folder where reports will be stored on the SD card and to also specify a Gmail account and mail subject if the report is to be sent to a remote recipient or possibly server for analysis.

d) Feature Vectors

Analysing activities of the system will give an accurate representation of the behaviour of the applications. The aim of intercepting these activities is to create an output file containing the events generated by the Android applications. This file provides useful information such as opened and accessed applications, running applications, running services, timestamps, received SMSs, sent SMSs, calls received, calls initiated and device status as at the time of occurrence of the activity. This information generated by the Device Monitoring application is used to represent the behaviour of applications.

IV. Discussion of Result

A sample report obtained from a single run of the feature extraction model implemented as a Device Monitoring application is given and discussed here.

```
before,Facebook,0,0,0,0,1,?
before,Messages,0,0,0,0,1,?
before,com.mediatek.voicecommand.service.VoiceCommandManagerService,0,0,0,0,1,?
before,com.mobogenie.service.WifiUpdateService,0,0,0,0,1,?
before,ua.com.doublekey.devicemonitoring.ServiceMonitoring,0,0,0,0,1,?
before,com.mobogenie.service.CommonService,0,0,0,0,1,?
before,com.mediatek.CellConnService.PhoneStatesMgrService,0,0,0,0,1,?
before,com.tecno.ime.IME,0,0,0,0,1,?
before,com.mediatek.filemanager.service.FileManagerService,0,0,0,0,1,?
before,com.mobogenie.service.MobogeniePushService,0,0,0,0,1,?
before,com.afmobi.palmchat.LaunchService,0,0,0,0,1,?
before,com.whatsapp.messaging.MessageService,0,0,0,0,1,?
before,com.mediatek.FMRadio.FMRadioService,0,0,0,0,1,?
before,com.facebook.push.mqtt.service.MqttPushService,0,0,0,0,1,?
before,com.mobogenie.service.MobogenieService,0,0,0,0,1,?
before,com.mobogenie.plugin.cys.cleaner.service.BackgroudCheckService,0,0,0,0,1,?
07.10.2015 20:36:47,com.facebook.fbservice.service.DefaultBlueService,0,0,0,0,1,?
07.10.2015 20:36:47,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:36:50,com.facebook.vault.service.VaultManagerService,0,0,0,0,1,?
07.10.2015 20:36:52,com.facebook.analytics.service.AnalyticsService,0,0,0,0,1,?
07.10.2015 20:37:50,com.facebook.fbservice.service.DefaultBlueService,0,0,0,0,1,?
07.10.2015 20:41:07,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:41:15,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:42:24,Launcher,0,0,0,0,1,?
07.10.2015 20:42:36,YouTube,0,0,0,0,1,?
07.10.2015 20:45:35,Launcher,0,0,0,0,1,?
07.10.2015 20:45:38,Google Play Store,0,0,0,0,1,?
07.10.2015 20:45:44,Launcher,0,0,0,0,1,?
07.10.2015 20:45:48,Gallery,0,0,0,0,1,?
07.10.2015 20:47:55,Launcher,0,0,0,0,1,?
07.10.2015 20:48:02,Torch,0,0,0,0,1,?
07.10.2015 20:48:05,Launcher,0,0,0,0,1,?
07.10.2015 20:48:18,Contacts,0,0,0,0,1,?
07.10.2015 20:48:32,?,1,0,0,0,1,?
07.10.2015 20:48:32,Phone,0,0,0,0,1,?
07.10.2015 20:49:27,Contacts,0,0,0,0,1,?
07.10.2015 20:49:29,Launcher,0,0,0,0,1,?
07.10.2015 20:49:32,Email,0,0,0,0,1,?
07.10.2015 20:51:12,Launcher,0,0,0,0,1,?
07.10.2015 20:51:20,SendSMS,0,0,0,0,1,?
07.10.2015 20:51:20,?,0,0,0,1,0,?
07.10.2015 20:51:32,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:51:40,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:51:57,?,0,1,0,0,1,?
07.10.2015 20:51:57,Phone,0,0,0,0,1,?
07.10.2015 20:52:01,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 20:58:48,Launcher,0,0,0,0,1,?
07.10.2015 20:58:49,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 21:07:04,WhatsApp,0,0,0,0,1,?
07.10.2015 21:08:52,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 21:09:40,com.facebook.conditionalworker.ConditionalWorkerService,0,0,0,0,1,?
07.10.2015 21:13:08,Tecno Input,0,0,0,0,1,?
07.10.2015 21:13:10,WhatsApp,0,0,0,0,1,?
07.10.2015 21:16:12,Launcher,0,0,0,0,1,?
07.10.2015 21:16:28,SendSMS,0,0,0,0,1,?
07.10.2015 21:16:53,Launcher,0,0,0,0,1,?
07.10.2015 21:16:59,Device Monitoring,0,0,0,0,1,?
```

07.10.2015 21:17:00,Monitoring Stopped
Tally:,,out calls: 1,in calls: 1,out sms: 0,in sms: 1

The report shows the date and time the Monitoring Device application was started. Immediately after that line is the field or attributes of the collected information in a CSV manner. After the attributes are the attribute values entered in the order of the specified attributes. The first attribute is the Date/Time, followed by AppName, OutCall, InCall, OutSMS, InSMS, Screen, and finally the Class in that order. For applications and services running before the Monitoring Device application was started, the Date/Time stamp is indicated as "before" while the applications and services started after the Monitoring Device application was started, the date/time stamp is indicated.

It is indeed very difficult to know which application performs a given activity since certain tasks are deprecated at application layer. Therefore, any activity that occurred without knowing which application perform the activity is given '?' as the value for the AppName attribute at that point. For the OutCall, InCall, OutSMS, InSMS and Screen attribute, the attributes have Boolean values; the value 0 is entered to represent the absence of the attribute and 1 is entered to represent the presence of that attribute. For the Screen attribute that represents the device status which is either idle or active, the value 1 means that the screen is in 'ON' or active state while 0 imply 'OFF' or idle state. Finally, the last attribute Class is not actually extracted from the applications or services by the Device Monitoring application but appended to the log file to indicate the class after classification is done using the classifier. Since the classification has not yet beencarried out on the data, the classes of the instances are undetermined and so they all have the value of '?' that means unknown class (normal or malicious).

When the Device Monitoring application is stopped, the event together with the Date/Time stamp of the event is registered and finally the report gives a summary of all the events in the form of count or tally.

V. Hardware and Software

The experiments were run on a laptop machine with the Intel Core-i3 -370M Processor, 3GBof available memory and 500GB Hard Disk Drive (HDD). This machine runs Windows 7 Operating System while Android Studio 1.2.2 Integrated Development Environment (IDE) was used as the Software Development Kit (SDK).

VI. Summary and Conclusion

In this paper, we describe the development of a feature extraction model that is used to extract Android application behaviour for anomaly malware detection. The type of information that can be extracted depends on whether the device has been rooted or not. Our focus is on unrooted Android devices and the information that were extracted and used to describe Android application behaviours include date/time stamp of the running application and services given as Time, Application and service name (AppName), Outbound call (OutCall), Inbound call (InCall), Outbound SMS (OutSMS), Inbound SMS (InSMS) and the device status (Screen). The device status indicates whether there is an active interaction with the device by the user or not. When the screen is active (value of 1), it means there is active interaction with the device by the user and when the screen is idle or hibernated, it implies no active user interaction. Activities like sending SMS and initiating calls requires active user interaction. If these attributes have values of 1 when the screen state is idle (value of 0) implies a suspicious or malicious behaviour is taking place on the device by an application.

Although other features could be added, these were used as a test base to realise the concept of anomaly detection system. As earlier stated, the type of information that can be intercepted depends on whether the device is rooted or not. Rooting a device is a bridge of security and therefore opens up the device to attacks. Since the aim is to improve security of mobile devices and applications with Android platform, an unrooted device is used. To be able to access more information that could be used to describe application behaviour for anomaly detection purposes, it is recommended that access to certain information like system calls, network traffic etc. which are presently deprecated in unrooted Android systems should be allowed access by Google in some ways.

References Références Referencias

1. Abela Kevin, Joshua AngelesL., Don Kristopher E., Delas Alas, Jan Raynier P., Tolentino, Robert Joseph and Gomez, Miguel Alberto N. (2013). An Automated Malware Detection System for Android using Behavior-based Analysis AMDA. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 2 (2), pp 1-11 *The Society of Digital Information and Wireless Communications.*
2. You Joung Ham and Hyung-Woo Lee (2014). Detection of Malicious Android Mobile Applications Based on Aggregated System Call Events. *International Journal of Computer and Communication Engineering,* 3 (2), pp 149 -154, March 2014.
3. Ham Y.J., Choi W.B., Lee H.W., Lim J.D. and Kim J.N. (2012), Vulnerability monitoring mechanism in Android based smartphone with correlation analysis on event-driven activities" *2012 2nd International Conference on Computer Science and Network Technology*, pp. 371-375.
4. Wu D.J., Mao C.H., Wei T.E., Lee H.M. and Wu K.P. (2012), Droid Mat: Android Malware Detection

through Manifest and API Calls Tracing, *7th Asia Joint Conference on Information Security*.

5. Wei T.E., Mao C.H., Jeng A.B., Lee H.M., Wang H.T. and Wu D.J. (2012), Android Malware Detection via a Latent Network Behaviour Analysis, *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*.
6. Burquera I., Zurutuza U. and Nadjm-Tehrani S. (2011). Crowdroid: behavior-based malware detection system for Android, Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, pp. 15-26.
7. You Joung Ham, Daeyeol Moon, Hyung-Woo Lee, Jae Deok Lim and Jeong Nyeo Kim (2014). Android Mobile Application System Call Event Pattern Analysis for Determination of Malicious Attack. *International Journal of Security and Its Applications* 8(1), pp.231-246, http://dx.doi.org/10. 14257/ijsia. 2014.8.1.22
8. Zack, Islam (2012). *Google Play Matches Apple's iOS With 700,000 Apps.* Businessweek, 30 October 2012. Retrieved fromhttp://www.tomsguide.com/us/Google-Play-Android-Apple-iOS,news-16235.html
9. Dini, G., Martinelli, F., Saracino, A. and Sgandurra, A. (2012). MADAM: A Multi-level Anomaly Detector for Android Malware. *Computer Network Security, Lecture Notes in Computer Science*, 7531, 240-253.
10. YousraAafer, Wenliang Du, and Heng Yin, (2013). Droid APIMiner: Mining API-Level Features for Robust Malware Detection in Android. pp 1-18. Retrieved from http://www.google.com
11. Luoxu Min and Qinghua Cao, (2013).Runtime-based Behaviour Dynamic Analysis System for Android Malware Detection. pp. 1-4. Retrieved from http://www.google.com
12. Ying-Dar Lin, Yuan-Cheng Lai, Chien-Hung Chen, and Hao-Chuan Tsai (2013). Identifying Android Malicious Repackaged Applications by Thread-grained System call Sequences, *Elsevier:Computers & Security*, pp 1-11, (2013), http://dx.doi.org/10.1016/j.cose.2013.08.010
13. Lovi Dua and Divya Bansal (2014).Taxonomy: Mobile MalwareThreats and Detection Techniques. *Dhinaharan Nagamalai et al. (Eds) : ACITY, WiMoN, CSIA, AIAA, DPPR, NECO, In WeS–*2014 pp. 213–221.
14. Aswathy Dinesh (2013). An Analysis of Mobile Malware and Detection Techniques. pp 1-13. Retrieved from http://www.google.com
15. Tchakounté F. and Dayang P. (2013). System Calls Analysis of Malwares on Android. *International Journal of Science and Technology* 2(9), pp 669-674 September, 2013.
16. Muhammad ZuhairQadir, AtifNisar Jilani, and Hassam Ullah Sheikh (2014). Automatic Feature Extraction, Categorization and Detection of Malicious Code in Android Applications. *International Journal of Information & Network Security (IJINS)*3(1), pp. 12~17, February 2014.
17. Srikanth, R. (2012). Mobile Malware Evolution, Detection and Defense. *Unpublished Term Survey Paper*, *Institute for Computing, Information and Cognitive Systems*, University of British Columbia, Vancouver, Canada.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey in Wireless Ad Hoc Network Security and Secure Energy Optimization Approaches for Routing

By D V Srihari Babu & Dr. P Chandrashekhar Reddy
JNTUH, Hyderabad, India

Abstract- Wireless ad hoc network nodes together establish a network infrastructure without using any access points or base stations for communicates using multi hop schemes. It has significant characteristics like dynamic topologies, constrained in bandwidth and limited resource a high challenge in implementing security with optimized energy resource utilization which is the key aspects while designing modern ad hoc networks architecture. Ad hoc Networks nodes are limited in broadcast range, and also their capabilities of computation and storage are well limited to their energy resources. This limitation of resources in wireless ad hoc creates high challenges in incorporating security mechanism for routing security and privacy maintenance. This paper investigates the various issues and challenges in secure routing and energy optimization during communication in wireless ad hoc network towards security and secure energy utilization improvisation.

Keywords: *wireless ad hoc network, routing, security, energy resource optimization.*

GJCST-E Classification : *C.2.1 C.2.2*

Strictly as per the compliance and regulations of:

A Survey in Wireless Ad Hoc Network Security and Secure Energy Optimization Approaches for Routing

D V Srihari Babu [α] & Dr. P Chandrashekhar Reddy [σ]

Abstract- **Wireless ad hoc network nodes together establish a network infrastructure without using any access points or base stations for communicates using multi hop schemes. It has significant characteristics like dynamic topologies, constrained in bandwidth and limited resource a high challenge in implementing security with optimized energy resource utilization which is the key aspects while designing modern ad hoc networks architecture. Ad hoc Networks nodes are limited in broadcast range, and also their capabilities of computation and storage are well limited to their energy resources. This limitation of resources in wireless ad hoc creates high challenges in incorporating security mechanism for routing security and privacy maintenance. This paper investigates the various issues and challenges in secure routing and energy optimization during communication in wireless ad hoc network towards security and secure energy utilization improvisation.**

Keywords: wireless ad hoc network, routing, security, energy resource optimization.

I. Introduction

Ad hoc networks where all nodes cooperatively maintain network connectivity in multi-hop wireless networks. Networks of this kind useful for disaster relief and emergency needs through a temporary network connectivity which is required to be used in such situation. It enables communication between nodes by forward packets within each other's. Building such ad hoc networks creates many barriers imposed by the environment and significant technical challenge. Ad hoc network suffers due to high mobility and resource constraints in together. The multiple propagations and intervention in wireless transmission effects and provide wireless primarily on the limited primarily to the wireless medium, operating in an ad hoc network routing protocols combined to create significant challenges. Thus, in the field of lightweight equipment should be used. Because they run on battery lifetime and improve the network of battery life as they should be conserving energy resources.

Wireless mobile ad hoc network (MANET) due to its extensive features is widely used in many military and civilian applications. Ad networks collect data on many Military and civilian applications. Ad hoc networks collect data on many wireless applications that are designed for a variety of environments. Based on the assessment of the different categories of data in their intended application. The natures of the applications mentioned above are used by governments, and individuals concerned. However, data used in among are confidentiality, authenticity and availability must be maintained in the integrity of certification.

Security and resources effect sensors in wireless networks due to its very limited resources of wireless networks and other challenges [3][4]. Mobile ad hoc network operate on traditional security networks services due to the limitations of wireless sensor networks and its difficulties to employ traditional security measures. For example, it is inefficient to employ SSL protocol. SSL protocol for wireless sensor networks, inefficient as it requires a high amount of energy [5][6].

This paper provides an in depth investigation in security issues and secure energy optimization approaches in Wireless mobile ad hoc network. It initially discusses the trends and mechanism of mobile ad hoc network communication in Section-2. Security issues and vulnerabilities are being discussed in section-3 and the energy optimization for longer network stability is discussed in Section-3.

II. Wireless Mobile ad hoc Network

A mobile ad hoc network (MANET) is dynamic arbitrary and temporary network topology to manage the wireless mobile nodes with self-configuration. People and vehicles using the first wireless communication infrastructure or the infrastructure of such areas without the need for an extension can internetwork [3].

All the nodes in Mobile ad-hoc network communicate directly to their range nodes which are in their radio range. Direct communication to communicate with each other within the intermediate node (s), while that of the nodes. In both cases, all nodes are involved in communication with the wireless network automatically, so this can be seen as some kind of mobile ad-hoc network.

Mobile ad hoc network are able to communicate directly to all the other titles in the radio range coverage. To communicate with each other in direct communication range, inter-node (s) that do not

Author α : Assoc. Professor, Dept of ECE Kottam karunakara Reddy inst. of Technology, Kurnool Andhra Pradesh, INDIA-518218.
e-mail: srihari2k1@gmail.com
Author σ : Professor, Department of ECE JNTUH, Hyderabad.

use the neighbor information. In both cases, all the nodes will automatically participate in the wireless communication network can be seen as a mobile ad hoc network as a wireless form. It shows the following unique characteristics [4] as follows:

- Wireless links between nodes that are volatile and unpredictable. As well as the mobility of wireless nodes and nodes with limited power supplies, mobile ad-hoc network of wireless communication links between them involved nodes are not stable.
- Topology dynamic behavior is due to the continuous motion of the nodes, the constant changes in the mobile ad-hoc network topology. The other nodes in the network nodes and part-time into constant move out of radio range, and routing information is changing all the time because of the movement of the nodes.
- Statically configured not to the lack of robust security features in the wireless routing protocol is intended for ad-hoc environments. Ad hoc networks are constantly changing the topology of the routing protocol, because statically configured so as to prevent the kind of attacks and potential attacks to try to make use of every pair of adjacent nodes for routing to incorporate the issue for the need.

The above mentioned features are the traditional mobile ad hoc networks. Wired trend indicates malicious behavior suffers more than the network. Therefore, we must focus more attention to utilization of energy security and security issues in mobile ad hoc networks.

III. Limitation in Securing Manet Networks

MANETs are of much more risk than the network attack mechanism should proceed [2][17]. This is due to the following reasons.

a) Lack of Infrastructure

Ad hoc networks, certification authorities, and the line of servers do not apply to any classical solutions based on any infrastructure to operate independently.

b) Inadequate Physical Security

Mobile wireless networks are more vulnerable to physical security threats, fixed wireless networks, more than the average. Theft, spoofing, and DoS attacks should be carefully considered which are likely to increase. Already the most demanding security systems link security threat reduction wireless networks.

c) Limited Power Supply

Due to the temporary movement of network nodes, the node depends on the battery system for their energy supplies. The power supply can be limited because of denial-of-service attacks and selfishness.

d) Frequent Varying Network Topology

Arbitrary nodes are free to move anywhere. Incidentally network topology change and their distance from other nodes may have no limits. As a result of this spontaneous movement, the reaction gradually makes unidirectional links between nodes as well as to give rise to two directional changes in an unpredictable manner [5].

IV. Different Approaches in Manet for Security

Many different suggestions exist in the literature [17][18][19][20] but how to protect the environment of MANET. Many use cases or the environment can be used only for specific solutions, but protocol of bootstrapping the defense should be able to connect to the network, especially in settings where new issues are arise any time and maintain it is a difficult question. In short, this section will be present to establish securities which are already known.

a) Distributed Security Approach

With the fully distributed gateway to access any server nodes or MANETs, completely self-organized security solutions [16] will be used. Each node in a local public key is to manage the repository. Repositories available can be found using a certificate chain to validate a certificate.

The certificate authority using secret sharing method or action can be decentralized. Using this technique makes it possible to distribute several nodes on a common centralized authority. Many nodes distribute a secrete and deals only through cooperation, can the secret reunion. Unfortunately, this method can be a Sybil attack.

b) Location Dependable Security Approach

Taking advantage of the limited mobility or using localized node in a mobile ad hoc network, the security of the communication paths is introduced to the other possibilities. The so-called imprinting of a security in relation to the use of the direct physical contact. This approach is extended by Balfanz et al. [1] and they propose that the public key certificates to the exchange location-limited channel. In some applications, such as ad-hoc communication with a printer and the use of the bootstrap method is very simple security policy. Because of the mobility of the nodes, this approach increases the distribution network within the security association. For self-organized networks this method is exclusively appropriate.

c) Broadcast Solutions

Mobile ad-hoc network is also supported by the existing transmission networks. The distribution networks of the media (audio and video), but also the data for the channels are made. This data is sent over the secure channel, broadcast encryption schemes are

very useful. If the receivers had previously applied to be included in the information packets for transmission encryption to decrypt and access the data. Broadcast encryption also allows you to remove or exclude former recipients from future broadcasts and data can be encrypted using a symmetric encryption key. We also know that a valid key is used in many different keys encrypted with the receivers. Nodes in the network are transmitted in encrypted keys to a key management block, are stored in. The key to decrypt the data nodes and the maintenance of a credible process to extract the block. The transmission encryption in the sense of broadcast it is introduced in [6]. Displayed little change in the policy of this that allows the user to set up groups [11]. Therefore, only a certain number of senders and receivers of messages can be creating as readable.

d) Trust and Reward Procedures

In a wireless network selfish nodes do not support which generally cause the problem for network performance disruption to MANETs. Support and participation are more attractive and a really good way to have been proposed [14]. The node can participate in a lot of debt often, than not presented any packet nodes. The recompense scheme also drives like operations, e.g. links can often present path for packet headers which will be expressed in more interest. Therefore, the network will be increased confidence. These can be used to secure many other protocols and mechanisms for the MANETs.

V. Security Countermeasure Approaches in Manet

To provide secure communication between the nodes to communicate security is a primary concern in MANET. To provide solutions to the problems involved in the security of mobile networks, we should be able to explain to the two most commonly used methods. Prevention of basic network functions in the early stages of their design is not embedded in the network operation which can be easily threatened.

a) Prevention Mechanism

Prevention of discontent from malicious attacks, such a solution is described by initiating active nodes. In the absence of infrastructure it is difficult to provide prevention using the policies of authentication, access control, encryption and digital signature policy, and also by using traditional methods one can provide the first line of defense. Such tokens or smart card PIN, phrases or used in addition to verification of biometrics is available through some security modules.

b) Reactive Mechanism

Identifying malicious activities and taking actions in reactive protocols mechanisms specifies any evidence of malicious that tries to take punitive measures against the reactive approach. MANET intrusion detection system (IDS) is to support schemes such as the use of enforcement mechanisms, etc. These intrusion detection systems are used to detect the manipulation and disorders. Such as Nuglets, confidant, CORE and selfish node behavior to reduce the implementation of cooperation, such as token-based. In this category, they will be able to recognize and react to the threat of such applications is the ability to induce all the protocols.

c) Security Schemes in Ad hoc Networks

In malicious network activity and specific issues related to the environment it is difficult to distinguish between in ad hoc networking. An ad hoc network malicious nodes at random intervals is to enter and leave as soon as the radio transmission range to avoid detection or disrupt network activity may collude with other malicious nodes. Further complicating the detection of malicious nodes behave only occasionally harmful. In order to get a global view of the network topology makes it difficult to dynamically and quickly, which is expected to become obsolete. In order to achieve the security objectives of many security schemes to succeed, even though none of them ad hoc wireless networks, security aspects of the proposed deals

i. *Intrusion Detection*

Intrusion audit data provide evidence Detection System [17] for capturing the attacks. Based on the audit data type used, intrusion Detection System can be classified as a network-based and host-based. Means of network packets through the network hardware interface former usually runs in the second Test monitors and analyzes events and hospitality programs or users [18].Manipulation detection (use patterns of known attacks) and abnormal detection (known attacks deviation flag): intrusion detection systems can be classified as the methods used. Both methods rely on the use of those packets for packets sniffing and analysis [19].

Zhang and Lee [17] described each node in a wireless ad hoc network IDS intrusion detection and personal responsibility by agents involved in the name of the proposed architecture for intrusion detection and response. It can monitor real-time traffic which has no fixed "focus points" Because, audit collection devices is limited by the range of the radio. Anomalies wireless ad hoc network anomaly detection schemes is expected to be localized, incomplete and possibly from the old information is not easily distinguishable. Therefore, the authors [17] of agents based IDS has proposed a new structure in intrusion detection network to improve security, such as encryption, authentication, secure MAC, security, routing and intrusion prevention techniques, complements. Effective, distributed and collaborative construction and preferably it should have been implemented in the detection of an anomaly. If all

the networking layers and incorporated into the further development of a comprehensive, cross-layer approach can be achieved.

ii. *Secure Routing in Wireless Ad hoc Networks*

Wireless ad hoc networks routing and wire-line networks cannot rely on dedicated routers. This functionality is simple terminals, as well as routers for other nodes that work is spread out over all the nodes. Data routing face many problems, such as providing a secure environment for networking and for the purposes of possible security attacks experienced temporary special. Ad hoc networks are the most popular routing protocols do not comprise of security aspects. Ad hoc wireless networks from security attacks, and especially attacks at the network layer of the defense, some of the requirements [20] should fulfill. Complete missions and the threat of a temporary wormhole attack against the disabled can disrupt communications. Based on the identification of a number of proposals for the use of wormhole packets.

Different approaches are very security-conscious in wireless ad hoc networks which have been proposed to achieve the security. In Table -1 it shows the most important security-strengthening properties awareness which drives the appropriate techniques to solve the following implementation for the various mechanisms of security aware routing protocols (SWRP).

Table 1 : Secure aware routing properties and techniques

Authenticity	Password, certificate
Authorization	Credentials
Integrity	Digest, digital signature
Confidentiality	Encryption
Non-repudiation	Changing of digital Signatures
Timeliness	Timestamp
Ordering	Sequence number

Many security routing protocols are discussed briefly in the following subsections.

SRP: Secure Routing Protocol (SRP) [21] is regarding the information to disrupt the process of the discovery, the acquisition of the guarantee to protect against attacks that can be applied to a multitude of reactive routing protocols. Either way, replies to compromise or be rejected again or ever reach the node back to the trial, the fabrication are protocol guarantees.

SAR : This protocol[22] aware of the ad hoc routing protocol security metric to define the level of trust and security attributes which are taken into account in the routing. And significant levels of trust in the hierarchy of levels of trust between the nodes can be defined. Nodes with the high level of trust among themselves and with the distribution of a common key encryption / decryption keys for the Notes equal to the share of each trust level. However, the contract for a different level of security in the network increases the total number of keys to different keys.

SEAD: It is an efficient ad hoc distance vector operation for safe destination protocol-distance gradient vector. Vector creates DOS attacks and resource calculation (DSDV) drives Protocol [23] is based on. SEAD DSDV-SQ Operation protocol and the sequence number and operating table update message was inspired to deal with attackers that different industry metric. To secure this DSDV-SQ [24] operation protocol of SEAD not rely on each side to implement and expensive asymmetric cryptographic hash chain on art. SEAD operation using a hash table implemented security mechanisms chain features updated message sequence number and the metric is correct. The implementation mechanism to ensure the identity of the client, or the broadcast authenticates the sender information on SEAD attempt to remove malicious nodes.

ARAN: Depending on the situation ARAN cryptographic certificates, temporary ad hoc networks and the power of the routing protocol is to prevents from the malicious activities with the support of an trusted third party. Minimum safekeeping policy, reliability of messages, identity authentication and non-repudiation of a necessary from end-to-end authentication for passed and initial certification process implementation [25].

ARIADNE: On-demand safe operation Protocol of this is DSR-based highly efficient symmetric cryptography [26] only stay on. Protocol required that a genuine key to our view that this must be some. Each node of the network is the same in each of the authentic and genuine way of finding each chain element nodes to nodes (a node between the source and) must share a secret key. ARIADNE message authentication code (MAC) and the joint chief operating point provides authentication message. However, except for the higher version, wormhole does not protect against attacks.

S-AODV: Security-aware AODV protocol single malicious nodes [27] Therefore, efficient solution to eliminate the black hole attack. Malicious intermediate nodes, it was the shortest route to the destination because of advertising that black-hole problem. Or dealing with the limited means of generating e-solutions proposed by malicious packets to an intermediate node has been tested by the neighbors realized. S-AODV Protocol each intermediate node can be assumed that all transit operators ensure packets. Control Message Originator of South Africa's signature and the final part of the hash chain appends. Network cryptographically signed message headers and the second and intermediate

hash confirmed. 'S-AODV is unable to deal with malicious headers to control the working group, including a significant overhead.

VI. Secure Energy Optimization Routing in Wireless Communication

Internal attacks are ineffective or compromised nodes before using a global shared key security structures. Therefore, fair wormholes and internal attacks to identify more sophisticated security mechanisms, and to protect the malicious headers. Safe and secure operation routing that can be used to enhance the security WSN. In this section, we have selected the operation of routings for secure networks. Parts in the preceding are well know for the power of information solutions to the solutions.

a) SERP: Secure Energy Efficient Routing Protocol

Wireless Sensor Networks routing protocol for the safe, energy efficient is described in SERP – Secure energy efficient routing [25]. The main objective of this protocol is to limited base station power requirement with authentication and confidential data from the sensors to provide a robust transmission. It is relatively static sensor devices which are deployed in densely dedicated to WSNs.

The three key aims were considered during the scheme of the SERP as follows

- To ensure the efficient transmission of power to the network is to know the structure, and the maximum lifetime to the end of the network.
- Secure communications nodes should be able to identify the incorrect intrusion reports.
- Strong and resilient transmission failure of any node can greatly hamper the performance of a network.

Energy savings mechanism based on the selected nodes are disabled transceivers radio. The two main states of the nodes in a network to perform: Non forwarding - forwarding transceiver, switch off - both transceiver and sensing devices which are switched. The backbone of the structure of the network, has been the assumption that all the headers are either directed or in non-states. But while the active sensing device nodes forwarding state of their radio transceivers. On the other hand, forwarding nodes keep both the radio and the active sensing device. All the nodes to perceive the environment, and in any event not later identify nodes forwarding the data to the base station via a selected route nodes and broadcast on their radio signal ranges.

b) EENC: Energy Efficiency Routing with Node Compromised Resistance

Node is compromised immunity is a novel energy efficient routing protocol proposed by K Lin et al [28] as EENC. It describes that EENC compromised nodes under the situation of bypasses and corresponding energy intake, improves the accuracy of the packets. Reinforcement knowledge established on ant-colony optimization routing tables are used to the complete. All nodes in the network are assigned with a trust Likewise, such as multiple behavior is based on the characteristics of the computed value. A one-hop neighbor of each node in a sensor network calculates the value of the trust. The idea of EENC is to provide security for low energy consumption and manage its energy resources.

This protocol EENC was evaluated through simulation. The performance metric to consider life and network packets correctly receives rate included. The EENC performance compared with other operations algorithms, i.e., DRP and MTRP are described [29] and presents the results of simulation of EENC operating through the trans- mission line can often compromised headers [29] EENC is to ensure that the energy efficiency performance was observed, that the estimated lifetime testing and successful packet delivery ratio and a higher DRP for more EENC received MTRP.

c) Location-based Power Conservation outline

In [17] Location Based Energy Conservation Program (LBPC) was discussed by authors. They suggested that the power consumption reduction algorithm in MANET. Such protocol transmission range of adjustment for the nearest neighbors is the first Hop neighbors and arbitrary detachment between the first uses of location information provided by GPS fitted to obtain general information about the distance. Two types of algorithms based on the results of the simulation are presented in the floods, which varied from 10-50% ratio showed an energy conservation. This is a significant amount of energy conservation, and the stored power adjustments as a result of a variety of network transmission range are done. However, the average distance to the neighboring transmission range is equal to the ratio of low to provide other performance parameters, but high in energy conservation.

d) SPAN: Energy Efficient Coordination Algorithm for Topology Maintenance

SPAN protocol, which reduces power consumption without reducing network connectivity also code named to ad hoc multi-hop wireless networks for the distribution of synchronization technique [18]. SPAN is coordinated by the cycle of “stay and sleep-awake" between the nodes and the ad-hoc multi-hop data packet performs routing within the network, while the other nodes are in power redeemable approach and occasionally to check if they will awaken and become a coordinator. During coordinator election every node in the network can adaptively become a coordinator and rotating them in time to decide whether or not to use a random back-off delay, the process is done by the SPAN. Back off delay for a node to other nodes in the neighborhood of the delay and the number of nodes is a function of the amount of remaining power. Network

connectivity not only is to protect the approach adopted in SPAN, it also preserves the ability to reduce latency and provides significant energy savings. Node density decreases only slightly increases as the size of the power saving provided by SPAN. Practically nodes wake up and listen for traffic from advertising in the current run of SPAN, features energy-saving, can be used [19].

e) Power-aware Routing Protocol

Power awareness Routing (PAR) [21] is maximizes the life span of the network and, hence, the source of the data packets transmitted during the process of setting up the route to the destination, choose less congested and more stable way to reduce power consumption by providing energy efficient routes. PAR protocols on the three parameters are the accumulated energy of a way, the status of the battery's life and the type of data to be transmitted. PAR time to focus on the core metrics are chosen path, hence, less traffic for the delivery of data is considered to be more stable. That provided different ways for different type of data transfer, network lifetime are increased. PAR simulation results from the energy-related performance metrics to the different ways in high mobility scenarios, such as DSR [22] and AODV [23] shows that outperforms the relevant protocol. However, PAR suffers increased latency during data transfer, but it goes a long way, and found enormous energy savings.

VII. Conclusion

In this paper, the mobile ad-hoc network routing security solutions in energy conservation issues and provides an overview of the study of the protocols. Due to the lack of infrastructure for wireless networks and the dynamic and transient nature of the relationship between network nodes, designers, especially prepared to impose additional challenges. Advanced security mechanisms, security must be designed to achieve the goals and they are effective. Ad-hoc functionality to provide a secure link layer security features are intended to be embedded in the equipment. Another challenge is preventing the efficient use of computing resources, computing harmful. Research in the field of authentication and key management to be efficient in terms of computational burden, which focuses on the design of the cryptographic algorithms. These protocols are available in various performance demands and proposals identified by the use of force against the parameters of this exhibition show the maximum effect. The study describes the achievement of high power conservation without compromising other performance metrics in MANET which provides for the performance demands of individual protocols. In the future, we intentionally designed to deliver the perfect blend of MANETs with some metrics for the performance demands with the intention to use the proposed protocols.

References Références Referencias

1. Patwardhan, A., Parker, J., Joshi, A., Karygiannis, A., and Iorga, M., "Secure Routing and Intrusion Detection in Ad hoc Networks," 3rd IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 2005
2. K. Sanzgiri, D.La Flamme, B.Dahill, B.N. Levine, C.Shields, and E.M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.
3. M. Rahman, S. Sampalli, and S. Hussain, "A robust pair-wise and group key management protocol for wireless sensor network," in GLOBECOM Workshops (GC Wkshps), 2010 IEEE, Miami, FL, 2010, pp. 1528-1532.
4. M. El-Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in Electro/Information Technology (EIT), 2012 IEEE International Conference on, 2012, pp. 1-6.
5. H. Soroush, M. Salajegheh, and T. Dimitriou, "Providing transparent security services to sensor networks," in Communications, 2007. ICC'07. IEEE International Conference on, Glasgow, 2007, pp. 3431-3436.
6. Anuradha Garg, Ajay Tiwari, Hemant Kumar Garg, "A Secure Energy Efficiency Routing Approach In Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) , Volume-2, Issue-3, February 2013
7. E. Niewiadomska-Szynkiewicz, P. Kwaœniewski, and I. Windyga, "Comparative study of wireless sensor networks energy-efficient topologies and power save protocols", J. Telecom. Inform. Technol., no. 3, pp. 68–75, 2009.
8. K. Sharma, M. K. Ghose, D. Kumar, "A comparative study of various security approaches used in wireless sensor networks", Int. J. Adv. Sci. Technol., vol. 17, pp. 31–44, 2010.
9. M. Ahmad, M. Habib, and J. Muhammad, "Analysis of security protocols for Wireless Sensor Networks", in Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011, Shanghai, China, 2011, vol. 2, pp. 383–387.
10. Perkins, C. E. and Bhagwat, P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of SIGCOMM 1994, 1994
11. Yi, S., Naldurg, P., and Kravets, R., "A Security-Aware Routing Protocol for Wireless Ad hoc Networks," 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002
12. Zhang, Y. and Lee, W., "Intrusion Detection in Wireless Ad hoc Networks," Mobicom'00, Boston, MA, USA, 2000

13. Wai, F. H., Aye, Y. N., and James, N. H., "Intrusion Detection in Wireless Ad- Hoc Networks," CS4274 Introduction to Mobile Computing, term paper, School of Computing, National University of Singapore, 2005.
14. Y.Sun, Z.Han and K.J.R.Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Communications Magazine, vol. 46, issue 2, pp.112-119, February 2008.
15. L. Gheorghe, R. Rughinis, R. Deaconescu, and N. Tapus, "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks," in Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, Nice, France, 2010, pp. 7-13.
16. Mike Burmester and Breno de Medeiros, "On the Security of Route Discovery in MANETs", IEEE Transactions On Mobile Computing,March 1, 2008.
17. E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," Aus CERT2006 R&D Stream Program, Information Technology Security Conference, May 2006.
18. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.
19. K.Sanzgiri, D.LaFlamme, B. Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.
20. Y.C.Hu, A.Perrig, and D.B.Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom'02, Atlanta, GA, pp. 12-13 September 2002.
21. B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.
22. D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to Strangers: Authentication in Ad hoc Wireless Networks. In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, February 2002.
23. Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietfmanet-olsr-11.txt, July 2003.
24. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks,. in Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.
25. J. Hall, M. Barbeau, and E. Kranakis, .Enhancing intrusion detection in wireless networks using radio frequency ngerprinting,. in IASTED International Conference on Communications, Internet, and Information Technology, 2004, St. Thomas, US Virgin Islands, 2004, pp. 201.206.
26. A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", Annales des Telecomm., pp. 529–541, 2008.
27. K. Lin, Ch. F. Lai, X. Liu, and X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks", Mob. Netw. Appl., vol. 17, pp. 75–89, 2012.
28. Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks", in Proc. 25th IEEE Int. Conf. Com. Commun. INFOCOM 2006, Barcelona, Spain, 2006, pp. 1–12.
29. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks", Wirel. Netw., vol. 8, no. 5, pp. 521–534, 2002.
30. C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", in Proc. 2nd Int. Conf. Embedded Networked Sensor Sys., Baltimore, MD, USA, 2004, pp. 162–175.
31. Ajina A, "Energy Efficient, Power Aware Routing Algorithm For Sensor Network". International Journal of Computer Theory and Engineering, Vol.3, No.1.1793-8201, February-2011.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Issues and Challenges in Congestion Adaptive Routing in Mobile Ad Hoc Network

By Govardhan Reddy Kamatam, Podili V S Srinivas & Chandra Sekharaiah K
Kottam Karunakara Reddy Institute of Technology Kurnool, India

Abstract- Mobile ad hoc networks is the future wireless communication systems have recently emerged as an important trend. Mobile adhoc network is self-configurable and adaptive. Due to the mobility of nodes, the network congestion occurs and it is difficult to predict load on the network which leads to congestion. Mobile adhoc network suffers from a severe congestion controlling problem due to the nature of shared communication and mobility. Standard TCP controlling mechanism for congestion is not fit to the dynamic changing topology of MANETs. This provides a wide scope of research work in mobile ad hoc network. The purpose of this survey is to study and analyze various issues and challenges in congestion control mechanisms in adaptive routing protocols in Mobile Adhoc Network (MANET).

Keywords: *manet, TCP, congestion control, adaptive routing, congestion detection.*

GJCST-E Classification : *C.2.6 C.1.3*

Strictly as per the compliance and regulations of:

A Survey on Issues and Challenges in Congestion Adaptive Routing in Mobile Ad Hoc Network

Govardhan Reddy Kamatam [α], Podili V S Srinivas [σ] & Chandra Sekharaiah K [ρ]

Abstract- **Mobile ad hoc networks is the future wireless communication systems have recently emerged as an important trend. Mobile adhoc network is self-configurable and adaptive. Due to the mobility of nodes, the network congestion occurs and it is difficult to predict load on the network which leads to congestion. Mobile adhoc network suffers from a severe congestion controlling problem due to the nature of shared communication and mobility. Standard TCP controlling mechanism for congestion is not fit to the dynamic changing topology of MANETs. This provides a wide scope of research work in mobile ad hoc network. The purpose of this survey is to study and analyze various issues and challenges in congestion control mechanisms in adaptive routing protocols in Mobile Adhoc Network (MANET).**

Keywords: manet, TCP, congestion control, adaptive routing, congestion detection.

I. Introduction

In recent times, there was a large leap in the field of development communication. Now, mobility communication has become one of the most needed. Mobile networks (MANETS) is one of the most mobile and flexible, powerful and effective way of communication. It is self-organized and configures itself on the fly. As it is lack of infrastructure these networks are quick to deploy environment and provide applications in diverse domains. Most commonly it is established for military areas, emergency and rescue operations, business applications and many more, just because they are economical.

In Adhoc networks routing protocols [4], it is necessary to use the potential of providing high-quality communication. There are a lot of network resources that limit the portability of the device, to manage the size and weight. Hence the need for the distribution of traffic between the mobile host nodes in the MANET suffers due to limited buffer, bandwidth, and battery power. In MANET routing protocol, the tasks should be distributed fairly between the mobile hosts.

Author α : Associate Professor, Dept. of C.S.E., Kottam Karunakara Reddy Institute of Technology, Kurnool, Andhrapradesh, India
e-mail: kamathamgovus@gmail.com
Author σ : Professor, Department of C.S.E., Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad.
Author ρ : Professor, Department of C.S.E. School of Information Technology, JNTUH, Hyderabad.

In wireless communication, devices will be equipped with the mobile hosts. The main features of MANET are self-configurable and deployable with multi-hop communication environments without a central coordinator. It faces frequent link breakage due to bandwidth, processing power, battery life, and resources such as mobility limitations. So this is fully distributed and often MANET positive changes in the topology of the routing protocol, often linked to the breakup of the major challenges.

II. Routing in Manets

Wireless network in disasters is to deliver information to law enforcement and the military to coordinate the distribution of mobile computers for many applications to provides quick access to information irrespective of the locations and distance. It was stated that, an adhoc assembly of wireless mobile hosts working deprived of the aid of any established infrastructure or centralized administration to make temporary communication [1].

In MANET routing structure depends on many factors, including the selection of routers, and finds a way to quickly and efficiently solving the basic and typical requests, which is to serve [6]. These networks are to guide the effective use of limited resources, the availability of the right-peer network, and therefore need to be motivated.

Also, most of the aggressive natures of these networks, which aim at achieving the stability of the routing protocols, are designed specifically for motivating the study of various protocols.

a) Classification of Routing Protocols in MANET

Routing protocols in MANET are classified based on the structure of the network and routing strategy. The flat routing, hierarchical routing and geographical position assisted routing are based on the structure of the network. Routing protocols are classified as table-driven and source routing protocols can be categorized based on the routing strategy:

i. *Proactive – Table driven Routing Protocol*

Proactive based routing protocols maintain regular and accurate information for data routing through periodical message exchange between the

nodes. Transmission of data to the destination node, the path can be calculated based on the routing table information. Keeping regular update of the routing information in this routing is an overhead in this protocol. A large number of dynamic topology update operation is required to turn adhoc wireless networks node mobility. Limited resources, bandwidth usage, and performance, has a negative impact on the wireless devices. This category of extension to protocols generally is wired operators protocols. For example: DSDV - Destination Sequence Distance Vector, OLSR - Optimized Links State Routing, WRP - Wireless Routing Protocol and many mores [2]. Without the need to find practical operation of the Protocol is the main advantage of adhoc network process, is always low as a result of periodic updates and overhead disadvantage of this operation and the main destinations are available to all protocols.

ii. *Reactive – On-Demand Routing Protocols*

Reactive protocols are termed as On-Demand routing protocols, it does not know the way to find a mechanism to node until a destination path for communicating with it has started. It can respond quickly to changes that could occur on the mobile ad hoc network nodes in their operation. Reactive carriers significantly lower than the cost, performing better than the practical operation of carriers and still less (or removed) to change the time or lower where network operators accessories are included. It is broadly classified into two main activities know as route discovery and route maintenance. Few examples of reactive routing protocols are DSR, AODV, TORA etc., and many discussed in literatures [3].

iii. *Hybrid Routing Protocol*

The proactive and reactive approach both form a hybrid routing, consisting of the ZRP - Zone Routing Protocol [7], CEDAR - Core Extraction Distributed Ad Hoc Routing. ZRP splits network into zones for the proactive and reactive routing. Protocol operating reactive operation protocol and the protocol in the directive of a dynamic protocol. When a node needs to send data to the destination in the region, and this directly to the proactive operation with carriers, when more information is already in the destination in tables. If operation of the source node is in the transmission line until it reaches the target area. The edge nodes in the target road send back a message by back route reply. It further noted the request referred to in any way address nodes. This information will be used to show the way back to the source. If broken links are found, the reconstruction does not exist locally, possible, and upgrade path will be sent to the source, or may be the first place to start to find the way to become global.

III. Transmission Control Protocol (TCP) in Manets

TCP and MANETs both are based on the transport layer protocol for communication but MANET follows multi hop communication for data routing [8][9]. It is the atmosphere of a traditional wired network between the hosts which provides a reliable end-to-end data delivery. TCP durability is achieved by retransmitting lost packets. Therefore, the estimated round-trip delay of each TCP sender and the average deviation derived from it maintains a running average. The sender receives a receipt if any within a specified timeout interval is retransmitted packets will be duplicated or received. Dependability on the tradition wired network, no packet loss due to congestion is an implicit assumption that the TCP is made. To reduce congestion TCP congestion control [10] [11] is used when packet loss is detected.

TCP is well tuned for many applications that support Web access, file transfer and e-mail, which has become the de facto transport protocol in internet. The Internet has its widespread use within the wireless networks and wireless networks TCP provides reliable data transfer services for wired communications across the Internet [12]. TCP for wired internet in order to extend the wireless world is crucial to be well over the wireless network types. Given the specific challenges of wireless, TCP behavior to understand and improve the performance of TCP over wireless networks, has been considerable research and proposed various schemes.

The investigation is still active in this area, and many issues are still wide open, in hopes that the good readers of TCP over wireless networks to pinpoint the primary cause of performance degradation and solution covering the spectrum is state of the art in understanding the problems and propose solutions thus improved on the basis of the current ones .

TCP as a Transport Layer Protocol perform the flow control, error handling and Congestion control, and the state of modern technology methods of retransmission and fast recovery of selected acknowledgment, and how quickly and efficiently respond to network congestion.

By examining the TCP's performance studies over MANETs we identified the following major problems:

- TCP accesses are not the way to distinguish between losses due to network congestion and route failures.
- TCP accesses frequently suffer from route failures.

a) Challenges in TCP Communication

Wireless ad hoc networks are some of the features [12] of TCP performance that will significantly deteriorate if they do not do anything. Basically, these features, such as channel burst errors, mobility and communication asymmetry.

i. *Channel Error*

In Wireless channels, due to multipath fading and shadowing, high bit error rate of transmission occurs and it can corrupt packet transmission and may lead to loss of TCP data segments or ACK packets. If it does not receive ACK within timeout retransmissions, TCP congestion window of the sender as soon as a section of the RTO to significantly reduce the number of back and retransmits and lost packets. Channel errors can cause intermittent congestion window size by the sender to remain low, leading to low TCP throughput.

ii. *Mobility*

Due to user mobility, Wireless networks are characterized by handoffs. Typically, handoffs may cause temporary disconnections, due to packet loss and delay. TCP congestion will suffer many losses and unnecessary congestion control mechanisms to deal with such calls. Handoffs are expected to occur more frequently in the next generation mobile network should be allowed to adapt to the increasing number of users of micro-cellular structure. TCP could be worse things that cannot gracefully handle handoffs. Similar problems may occur in wireless LAN, mobile users will encounter during user mobility which cause disruption of network access due to the communication range.

The TCP equation-based approach within the TCP-friendly congestion control methods described by D. Bansal et al. in [3], Y.R. Yang in [2] is a method that relies on the TCP throughput in a network path with certain loss rate and round-trip time (RTT). The TCP equation method has demonstrated a reasonably good performance for wired networks, however has been found to decrease the performance of mobile ad hoc networks that recently led to the research of TCP friendly congestion control schemes for avoiding TCP's retransmission strategy which is expensive or unnecessary in real-time multimedia streaming applications.

A method of Explicit Congestion Notification (ECN) proposed by K. Ramakrishnan et al. in paper [15] evaluates the network congestion state, by marking a bit in passing packets IP header by each router to determine the possibility of network congestion, simultaneously monitoring the routers queue size. In this Explicit Congestion Notification approach the congestion is detected quickly however it does not give information about the size of the congestion. So the systems with ECN experience issues similar to those caused by AIMD algorithm over MANET.

IV. Congestion Control in Manets

MANETs will be crowded with limited resources. This network of shared wireless channel interference and fading at the time of packet switching and dynamic topology leads Victims and bandwidth packet deterioration due to congestion caused, and therefore, the time and energy are wasted on its recovery. By avoiding traffic congestion know the protocol to avoid using the affected links. Recognizing the serious problems of congestion problems related to the throughput degradation and fairness are huge [16].

Congestion control is the main problem associated with the incoming traffic control in a telecommunications network. The sending packets to prevent a wide range of intermediate nodes and networks, traffic control to reduce the rate used for congestive beaten or link capabilities. Traffic patterns, traffic control and dependability of the place and the presence of discontinuous directly without intermediate nodes are added by TCP to manage the traffic control without a clear opinion [17].

The principles of conservation of the packet, the additive multiplicative decrease in the growth rate of the fixed network are sending. End flow control system, traffic control network, including basic techniques and resources to control or prevent a traffic based on network traffic [18].

Mainly due to the obstruction caused by the failure of the packet MANETs. Mobility and adaptive routing network layer protocol over a failure to control congestion involving packet loss can reduce. Non-adaptive traffic carriers and operators face the following difficulties.

- Heavy Delay: Congestion control mechanism takes more time to find all the traffic. Sometimes it is advisable to use of new routes in critical situations. The main problem is the delay in the on-demand routing protocol in search of route.
- Heavy Overhead: To discover new paths for the traffic control system, Congestion management mechanism efforts are needed for the processing and communication. Multipath-routing protocol for managing multiple ways, even in spite of the hard effort it takes new protocol.
- Heavy Packet Lost: After the traffic load identified packet can be lost. Reducing the transmission rate at the sender or dropping packets at the intermediate nodes or both techniques were applied to control congestion. High rate of packet loss results in small bandwidth.

A new self-tuning RED for congestion control and QoS improvement in MANET [19] proposed by Jianyong Chen et al. increases the performance of TCP-RED network. The effects of the packet size and random early detection (RED) parameters [20] on trTCM and srTCM for congestion control and QoS improvement in MANET is studied by Hesham N. Elmahdy et al.

V. Congestion Detection in Manets

Incoming traffic is much larger than the capacity of the network traffic in a network that may occur during the particular period. End of the main problems affecting the performance of the entire network congestion and retransmissions of packets of data loss are rising. Recovery always leads to waste of time and energy, traffic congestion, packet loss and bandwidth levels. A variety of network routing algorithms have been used to reduce congestion [1].

Congestion can be classified into four different types:

- Immediate Congestion: This congestion is caused by mild bursts, created naturally by heaviness of IP traffic.
- Standard congestion: Under the manner in which the traffic capacity of the network or hop will be engineering.
- Flash congestion: The traffic bursts from individual sources add up to create the hills, where significant packet loss in a highly utilized network overload often refers to the momentary periods.
- Spiky delay: This is a condition where the number of packets is transmitted for a long time - a few milliseconds to tens of seconds of the packets transport delay from the time that shoots up.

Accurate and efficient detection sensor networks traffic congestion control plays an important role. Power and low cost in terms of computational complexity is the need for introducing new methods of traffic detection. Several methods are possible [21].

Kumaran et.al [22] proposed "Early Detection congestion and control routing" known as EDAODV. It is well ahead in time, and bi-directionally describes the findings of a non-congest hour looks for an alternative route. Kumaran et.al also proposed EDOCR [22] as "Early congestion detection and optimal control routing". It's rare in the general neighborhood, and network nodes and dense phases are separated, density of the network nodes are separated and a non-busy looking for an alternative way.

a) Buffer Queue Length

Queue length for traffic management is often used to identify the traditional data network. However, the queue length and link layer showed that the traffic indicator which can be used to link some of these applications can save weight for the indication of congestion and buffer utilization. It is based on buffer inductive functions traffic jam which is difficult to quantify the level of minimum or racing. Bimodal effect is responsible for the smooth and effective enough, and traffic control, to provide a very coarse [9].Peter Marbach [24] proposed a distributed scheduling and congestion control and QoS in the network for the development of active queue management mechanism for wireless adhoc networks based on a random-access scheduler.

For network congestions active-queue-management (AQM) strategies for managing traffic problems and a reduced effective buffer of a node based on prevention rules proposed by many researchers [25], such as RED [26] – "Random Early Detection", "Random Exponential Marking", etc. Braden proposed RED which describe the average size of the queue by monitoring the traffic of the future for the sake of the next generation Internet routers, among others, is approved by the IETF. Future study on buffer overflow traffic at the MAC layer and the network layer by supporting a non-traffic congestion problem by finding solutions that will give narrow solution. This strategy of avoiding or cutting of packet loss, delay and the amount of the reduction will be applied for improving the performance of the network.

An active queue management algorithm, termed as BLUE is proposed and evaluated by Wu-chang Feng, et al. [27]. The performance of blue is comparatively better than RED. Also another algorithm, Stochastic Fair BLUE (SFB) proposed for queue management use an infinitesimal amount of state information to identify and rate-limit nonresponsive flows.

b) Channel Loading

Channel load in the network is busy, but in fact, it provides detailed information about the local mitigation mechanism. Limited force, for example, the data traffic caused by the thrust generated by the high-level sources in large-scale congestion detection is low. Listening to channel a large part of the energy is consumed in a node [9].

In MANET networks, reducing the end-to-end delay and amount of traffic methods are proposed by Ehssan Sakhaee et al. [28]. Other benefits arising are linked to the duration of the growth, reduction in end-to-end delay, the less disturbance of the flow of data and lower path settings. In this mechanism, a new procedure is employed for route discovery unlike earlier reactive routing protocol in which only disjoint paths are chosen. A unique routing algorithm reduces the frequency of flood requests by extending the duration of the link.

VI. Congestion Problems in Manets

TCP provides a reliable communication link; because it uses the basic technique confirm data delivery, but more delay as compared to the UDP packet, so that if the sender share a common intermediate node, that congestion increases, and the maximum delay. A TCP packet loss due to congestion of the wireless channel errors, link approval, mobility and multi-path routing for mobile ad-hoc networks that can significantly harm because of an implicit supposition is invalid, TCP, networks (MANETs) mobile in the delivery of packages poorly run or disordered.

Adjusting the data rate used by each sender to avoid burdening the network with a network of shared resources is a necessary condition where multiple senders to fight for the channel capacity. Packets that cannot be transferred, removed when they arrive at the router. Accordingly, an excessive number of packets destined for the network bottlenecks leading to numerous discards the packet. These missing packets may have already passed a long path of the network, and thus, considerable resources are devoured. In addition, the transfer of power on even more lost packets, which is a sign of additional packets sent over the network. These factors result in a serious deterioration in the network throughput capacity and if the appropriate measures are not taken for the traffic control network congestion, resulting in the collapse and a zero delivery of data. This situation occurs at the early Internet, which leads to the development of the mechanism of congestion control TCP [8][18].

VII. Congestion Control Techniques for Adaptive Routing

Congestion adaptive routing protocol (CARP) that appears to control a route, will alert the node of congestion is likely to happen at all [29]. Thereafter, the node "bypass" in order to take a detour route to avoid congestion using non-congestion in the potential of the first node. When this happens, use the previous node a "bypass" the route to take a detour to avoid the potential overloading of the first non-congested node on the route. L. Shrivastava et al. [30] present a study of congestion adaptive routing protocols and congestion aware routing in DLAR - Dynamic Load-aware Routing, CADV - Congestion Aware Distance Vector, CARM - Congestion Aware Routing Protocol for different MANETs.

a) Congestion Monitoring

For a node to keep a check on the state of congestion, you can use a variety of metrics. Some key is the percentage of all queue length, packets retransmitted, standard delay and packets dropped. Increase of packet drop indicates that congestion is springing up. Either method can work virtually with CARP. The three levels of congestion that are more nodes and categorized as “red”, green” and “yellow” If a node from it being very busy, "yellow", "green" is free from congestion as "red" and more likely or already crowded.

b) Primary Route Discovery

Broadcaster receiver is to find a way to upgrade the receiver to transmit a package. REP packet sent by the sender to the receiver, which is the first copy, upgrade to meet. REP update before the return is the same way. This will be the primary route between the sender and recipient. Nodes along this route will be called as the first node. Both tactics are often employed by us to the discovery of the route to reduce traffic and provide advance hold on the congestion problems: (1) Upgrading dropped which already have a path to get to the destination, and (2) if it reaches a node is upgraded to a "red" status if a packet is dropped due to node congestion [29].

c) Traffic Splitting and Congestion Adaptability

The probability p of transmitting data from the beginning of the first link is set to 1, which must pass through each node. Periodic changes in the status of the next node based on the path congestion bypass overload. Congestion status of each node state funded pass-through. The important thing is that we must increase the amount of traffic on main line, if the main channel leading to less congestion and reduce a node.

d) Multi-path Minimization

The protocol is aimed at reducing the use of multiple ways to reduce the burden of CARP. P is the probability of the node to the next head long bypass overloaded or very busy, suggests that there is a way to send data over 1.0, if the base value is approaching. In this case, the bypass current node is excluded. The next primary node is too busy, then bypass routes or disabilities, as well as the main channel, will be required. CARP is only a pass-through to the nodes, the protocol is a very simple and light. Through the use of a bypass, burden is reduced because of the short length of the bypass. The first node must be connected to the bottom of each bypass the load after only a few hops, not a crowded place.

e) Failure Recovery

CARP elegantly and quickly take the help of a link to bypass the currently available that is capable of recommencing a popular routing protocol connectivity after breakage.

An end-to-end threshold-based algorithm developed by Mohammad Amin KheirandishFard et.al [31] improves congestion control and deals with link failure loss in MANET.A single queue variant of Start time Fair Queuing (SFQ), S-SFQ is proposed by Yuming Jiang et al. [32] which are accountability mechanism for the efficient flow control, congestion avoidance. RED and FIFO queue schemes as compared to other single-link the use of S-SFQ performance is superior flow constraints with respect and fairness.

Lijun Chen et. al. [33] proposed temporary traffic control for wireless networks, a combination of routing and scheduling. They refer to different types of networks and the ability to allocate resources in the network as the ratio between the generating utility problem previously with limitations, dual algorithm further increased to manage the network with a different channel and controlling device multi-rate for the high congestion control and quality of service in MANET.

VIII. Conclusion

In this paper we have explored the congestion control techniques used in mobile adhoc networks. Congestion in adhoc networks can be controlled either through routing or using the standard TCP congestion control mechanisms used in wired networks with modification and compatibility for wireless networks. Due to high node mobility and topology changes, the TCP control techniques applied to adhoc networks are inadequate to handle congestion. Heterogeneity of application scenarios does not let a conclusion and general-purpose solution for all possible scenarios of MANET applications. Thus, there is still considerable scope for solutions is open to solve problems of overloading and congestion issues. In future research work we will present a congestion prediction algorithm, a traffic data prioritization approach and a traffic normalization approach for congestion avoidance in mobile ad hoc network for achieving high quality of service, minimizing the delay.

References Références Referencias

1. D.A. Tran, H.Raghavendra, "Congestion Adaptive Routing in Mobile Ad Hoc Networks", IEEE Transactions on Parallel and Distributed Systems, 2006.
2. Y.R. Yang, M.S. Kim, and S.S. Lam. Transient behaviors of TCP-friendly congestion control protocols. Computer Networks, 41(2):193-210, 2003.
3. D. Bansal, H. Balakrishnan, S. Floyd, and S. Shenker. Dynamic behavior of slowly-responsive congestion control algorithms. In Proceedings of the 2001 SIGCOMM conference, volume 31, pages 263-274. ACM New York, NY, USA, 2001.
4. Muhammad Aamir and Mustafa A. Zaidi "A Buffer Management Scheme for Packet Queues in MANET", Tsinghua Science And Technology ISSNll1007- 0214ll01/10llpp543-553 Volume 18, Number 6, December 2013.
5. Amanpreet Singh, Mei Xiang, YasirZaki, "Enhancing Fairness and Congestion Control in Multipath TCP main technical program at IFIP WMNC'2013.
6. G.S.Sreedhar & Dr.A.Damodaram, "MALMR: Medium Access Level Multicast Routing for Congestion Avoidance in Multicast Mobile Ad Hoc Routing Protocol., Volume 12 Issue 13, pp.22-30, 2012.
7. K. Chen and K. Nahrstedt. Limitations of equation-based congestion control in mobile ad hoc networks. In Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on, pages 756 -761, 2004.
8. S.A.Jain and SujataK.Tapkir, "A Review of Improvement in TCP congestion Control Using Route Failure Detection in MANET., Network and Complex Systems, Vol 2, No.2, pp.9-13, 2012.
9. M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow. TCP Selective Acknowledgment Options. RFC 2018 (Proposed Standard), Oct. 1996.
10. Yung Yi and Sanjay Shakkottai. Hop-by-hop Congestion Control over a Wireless Multi-hop Network, 0-7803-8356- 7/04/$20.00 (C) 2004 IEEE.
11. Yi-Cheng Chan and Hon-JieLee,"A Hybrid Congestion Control for TCP over High Speed Networks. 2012 Sixth International Conference on Genetic and Evolutionary Computing. 2012.
12. Lien, Y.N., Hsiao, H.C.: A New TCP Congestion Control Mechanism over Wireless Ad Hoc Networks by Router-Assisted Approach. 27th IEEE International Conference on Distributed Computing Systems Workshops. (2007).
13. PurvangDalal, Nikhil Kothari and K. S. Dasgupta ,"Improving Tcp Performance Over Wireless Network With Frequent Disconnections. International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.6, November 2011.
14. Raffaele Bruno, Marco Conti, and Enrico Gregori ,"Average-Value Analysis of 802.11 WLANs with Persistent TCP Flows. IEEE Communications Letters, VOL. 13, NO. 4, APRIL 2009.
15. K. Ramakrishnan, S. Floyd, and D. Black. The addition of explicit congestion notification (ECN) to IP, 2001.
16. Soelistijanto B., Howarth M.P., Transfer Reliability and Congestion Control in Opportunistic Networks: A Survey. IEEE Communications Surveys and Tutorials, 2013.
17. Song W., Jiang S., Wei G., A Congestion-Aware Multipath Routing with Cross Layer Design for Wireless Mesh Networks. Proceedings of the 15th Asia- Pacific Conference on Communications, 2009, 157.
18. S.Rajeswari, Dr.Y.Venkataramani, "Congestion Control and QOS Improvement for AEERG protocol in MANET" International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 1, January 2012, pp.13-21.
19. WenyuCai, Xinyu Jin, Yu Zhang, Kangsheng Chen and Rui Wang, "ACO Based QoS Routing Algorithm for Wireless Sensor Networks" in Ubiquitous Intelligence and Computing, LNCS 2006.
20. Hesham N. Elmahdy and Mohamed H. N. Taha, "The Impact of Packet Size and Packet Dropping Probability on Bit Loss of VoIP Networks" in ICGST-CNIR Journal, Volume 8, Issue 2, pp. 25-29,January 2009.
21. S. Subburamm and P. Sheik Abdul Khader, "Efficient Broadcasting using Preventive Congestion Mechanism in Mobile ad Hoc Network., European Journal of Scientific Research, Vol.83, No.2, pp.302-313, 2012.

22. Kumaran, T.S. and V. Sankaranarayanan, 2010. Early detection congestion and control routing in MANET. Proceedings of the 7th IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN), Sept. 6-8, IEEE.2010
23. T. SenthilKumaran, V. Sankaranarayanan,"Early Congestion Detection and Self Cure Routing in Manet", Springer- Verlag Berlin Heidelberg, 2011.
24. Peter Marbach, "Distributed Scheduling and Active Queue Management in Wireless Networks" in INFOCOM 2007 :2321-2325.
25. Athuraliya, S., S.H. Low, V.H. Li and Q. Yin, REM: Active queue management. IEEE Networking., 15: 48-53. DOI: 10.1109/65.923940, 2001.
26. Braden, B., D. Clark, J. Crowcroft, B. Davie and S. eering et al., Recommendations on queue management and congestion avoidance in the internet. RFC, United States, 1998.
27. Wu-changFeng, et al, "The BLUE Active Queue Management Algorithms" proc. IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 10, NO. 4, AUGUST 2002.
28. Ehssan Sakhaee, et al, "A Novel Scheme to Reduce Control Overhead and Increase Link Duration in Highly Mobile Ad Hoc Networks" proc. reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.
29. Ikeda M., Kulla E., Hiyama M., Barolli L., Younas M., Takizawa M., TCP Congestion Control in MANETS Traffic Considering Proactive and Reactive Routing Protocols. 15th International Conference on Network-Based Information Systems, IEEE, 2012.
30. L. Shrivastava, G.S. Tomar, and S.S. Bhadauria, "A Survey on Congestion Adaptive Routing Protocols for Mobile Ad-hoc Networks", Int. Journal of Computer Theory and Engineering, vol. 3, Issue 2, 2011, pp. 189-196.
31. Mohammad Amin Kheirandish Fard, SasanKaramizadeh, Mohammad Aflaki, "Enhancing Congestion Control To Address Link Failure Loss over Mobile Ad-Hoc Network", International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.5, Sep 2011, pp.177-192.
32. Yuming Jiang et al, "On the Flow Fairness of Aggregate Queues" proc. 2011 Baltic Congress on Future Internet and Communications.
33. Chen, L., Lowy, S.H., Chiangz, M., Doyley, J.C.: Cross-layer Congestion Control, Routing and Scheduling Design in Ad Hoc Wireless Networks. Proc., IEEE, 25th International Conference on Computer Communication, INFOCOM. pp 1 - 13. (2007).

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Security of Elliptic Curve Cryptosystems - A Survey

By Koffka Khan
University of the West Indies, Trinidad and Tobago, W.I, India

Abstract- Elliptic curve cryptography or ECC is a public-key cryptosystem. This paper introduces ECC and describes its present applications. A mathematical background is given initially. Then its' major cryptographic uses are given. These include its' use in encryption, key sharing and digital signatures. The security of these ECC-based cryptosystems are discussed. It was found that ECC was well suited for low-power and resource constrained devices because of its' small key size.

Keywords: *elliptic curve cryptography; public-key; cryptosystem; security; rsa; el gamal; curve; key size.*

GJCST-E Classification : *C.2.0 D.4.6*

Strictly as per the compliance and regulations of:

The Security of Elliptic Curve Cryptosystems - A Survey

Koffka Khan

Abstract- **Elliptic curve cryptography or ECC is a public-key cryptosystem. This paper introduces ECC and describes its present applications. A mathematical background is given initially. Then its' major cryptographic uses are given. These include its' use in encryption, key sharing and digital signatures. The security of these ECC-based cryptosystems are discussed. It was found that ECC was well suited for low-power and resource constrained devices because of its' small key size.**

Index Terms: elliptic curve cryptography; public-key; cryptosystem; security; rsa; el gamal; curve; key size.

I. Introduction

Over the years, with the increase in processing power of computers, there has been a reduction in the work factor required to solve Integer Factorization (IFP) [17], [21], [3] and Discrete Logarithm (DLP) problems [6], [9], [18]. As a result, key sizes grew to more than 1000-bits so as to attain a reasonable level of security. However, in constrained environments carrying out thousand-bit operations is impractical. Therefore, a matter of growing importance in cryptography is the need for algorithms with low resource requirements [24], [14] that can be deployed on resource-constrained ubiquitous devices. This explains why other public-key methods would be welcomed, Elliptic Curve Cryptosystem (ECC) [12] being a probable candidate.

Elliptic curves are the basis for a relatively new class of public-key schemes. It is predicted that Elliptic Curve Cryptosystems (ECC) Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems in 1985, independently by Victor Miller and Neal Koblitz. Elliptic curve are not ellipse, but cubic curves. Properties of ECC made it stronger against various attacks in wireless sensor networks [7], RFID [8], smart card [20] and many others. It will replace many existing schemes in the near future. However, the complicated mathematical background of ECC results in more sophisticated algorithms. Mathematical basis for security of elliptic curve cryptography is computational intractability of elliptic curve discrete logarithm problem (ECDLP) [11].

Elliptic Curve Cryptography (ECC) can be applied to data encryption and decryption, digital signatures, and key exchange procedures. Every user has a public and private key. The public key is used for encryption or signature verification, while the private key is used for decryption or signature generation. ECC is used as an extension to current cryptosystems, for example, ECC Diffie-Hellman Key Exchange (EC-DH) [16], ECC Digital Signature Algorithm (ECDSA) [10] Elliptic Curve Integrated Encryption Scheme (ECIES) [23].

A motivation is given in Section II. In Section III a mathematical background is given. The major uses of ECC in present day cryptosystems are presented in Section III. The underlying theory of elliptic curve cryptosystems is discussed in section IV. Three ECC cryptosystems are given in section V. These are EC-DH, ECDSA and ECIES. The security of these cryptosystems are outlined in Section V with the advantages of using ECC. Finally the conclusion is given in section

II. Motivation

In order to understand the principle of asymmetric cryptography, the basic symmetric encryption scheme has to be recalled.

Figure 1 : Symmetric key encryption

Two properties are essential for symmetric key cryptosystems:

i. The same secret key is used for encryption and decryption.
ii. The encryption and decryption function are very similar (in the case of DES [5] they are essentially identical).

There is a simple real-world analogy for symmetric cryptography. Assume there is a safe with a strong lock. Only Alice and Bob have a copy of the key for the lock. The action of encrypting of a message can be viewed as Alice putting the message in the safe. In order to read, i.e., decrypt, the message, Bob uses his key and opens the safe.

However, there are several shortcomings associated with symmetric-key crypto-schemes.

Author: Department of Computing and Information Technology, The University of the West Indies, Trinidad and Tobago, W.I.
e-mail: koffka_@hotmail.com

- Key Distribution Problem. The key must be established between Alice and Bob using a secure channel. The communication link for the message is not secure, so sending the key over the channel directly can't be done.
- Number of Keys Even. Each user has to potentially deal with a very large number of keys. If each pair of users' needs a separate pair of keys in a network with n users, there are (n· (n−1)) / 2 key pairs. Thus, each user has to store n 1 keys securely. The number of keys that must be generated and transported via secure channels will become exorbitant.
- No Protection against cheating by Alice or Bob. Alice and Bob have the same capabilities, since they possess the same key. As a consequence, symmetric cryptography cannot be used for applications where we would like to prevent cheating by either Alice or Bob.

In order to overcome these drawbacks, Diffie, Hellman and Merkle made the following proposal. It is not necessary that the key possessed by the person who *encrypts* the message (that's Alice in our example) is secret. The crucial part is that Bob, the receiver, can only *decrypt* using a secret key. In order to realize such a system, Bob publishes a public encryption key which is known to everyone. Bob also has a matching secret key, which is used for decryption. Thus, Bob's key k consists of two parts, a public part, k_{pub}, and a private one, k_{pr} .

This systems works quite similarly to the good old mailbox system. Everyone can put a letter in the box, i.e., encrypt, but only a person with a private (secret) key can retrieve letters, i.e., decrypt (see Figure 1).

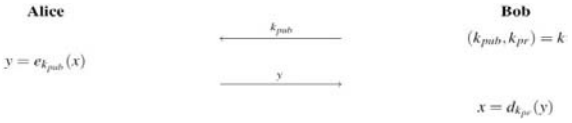


Figure 2 : Basic protocol for public-key encryption

By looking at that protocol the exchange of an encrypted key still remains a problem. This can be done by *encrypting a symmetric key*, e.g., an AES key, using the public-key algorithm. Once the symmetric key has been decrypted by Bob, both parties can use it to encrypt and decrypt messages using symmetric ciphers. But this still poses a grave problem for the public key sharing at the start of the protocol can be intercepted by Oscar. It is these security concerns that resulted in the need for the development of asymmetric cryptosystems.

Public key schemes are all built from one common principle, the one-way function.

Definition 1

A function f (x) is a one-way function if:

- y = f (x) is computationally easy, and
- x = f^{-1}(y) is computationally infeasible.

A function is easy to compute if it can be evaluated in polynomial time, i.e., its running time is a polynomial expression. In order to be useful in practical crypto schemes, the computation $y = f(x)$ should be sufficiently fast that it does not lead to unacceptably slow execution times in an application. The inverse computation $x = f^{-1}(y)$ should be so computationally intensive that it is not feasible to evaluate it in any reasonable time period, say, thousands of years, when using the best known algorithm.

Recently the key sizes of public key cryptosystems, for example, RSA prohibits their use in low-power, resource constrained computing devices. Due to this requirement ECC shows an advantage as much smaller key sizes (see Table 1) are needed for the same amount of security.

Table 1 Key sizes of ECC and RSA []

ECC(in bits)	RSA(in bits)
106	512
112	768
132	1024
160	2048
210	3072
283	7680
409	15360
571	21000

III. Mathemitical Background

In Section A modular arithmetic is described. Then, in section B integer rings is defined. Further, in section C finite fields is illustrated. In section D cyclic rings is explained. Section E portrays the concept of subgroups. In Section F the Discrete Logarithm in Prime Fields is depicted. Finally, in section G the Generalized Discrete Logarithm Problem is given.

a) Modular Arithmetic

Symmetric and asymetric ciphers are usually based on arithmetic with a finite number of elements. The sets of real and natural numbers are infinite. Consider a finite set of integers. The octal set of integer numerals are: {0, 1, 2, 3, 4, 5, 6, 7}. It is possible to do arithmetic in this set so long as≤0result ≤ 7. For instance: 2 x 2 = 4 or 3 + 4 = 7 is fine, but 7 + 5 gives 12. This result is not a subset of the octal set. To validate this operation an additional operator is used.

This is the modulus operation and is defined as follows:

Definition 2

Let p, r, q ∈ Z (where Z is a set of all integers) and q > 0. We write p ≡ r mod q, if q divides p− r. q is called the modulus and r is called the remainder.

Thus 7 + 5 = 12, which when divided by 8 (12/8) gives a remainder of 4. So 7 + 5 = 4 mod 8. In practice the integers involved have a length of 130–4096 bits so that efficient modular computations are a crucial aspect in modern cryptography.

b) Integer Rings

Consider the set of integers from zero to m-1 with two operators: addition and multiplication. A ring on this set is defined as follows:

Definition 3

A ring is the set of integers $Z_m = \{0, 1, 2, ..., m-1\}$ with the "+" and "×" operations $\forall\, e, f, g, h \in Z_m : e + f \equiv g \bmod m \wedge e \times f \equiv h \bmod m$

The following properties of rings are important:

- Closed: addition and multiplication of two numbers has a result in the ring.
- Ring operations are associative: $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c ∈ Z_m.
- A neutral element 0 with respect to addition, i.e., for every element a ∈ Z_m it holds that $a + 0 \equiv a \bmod m$.
- The additive inverse always exists for any element a in the ring, there is always the negative element –a such that $a + (-a) \equiv 0 \bmod m$.
- The neutral element 1 with respect to multiplication, i.e., for every element a ∈ Z_m it holds that $a \times 1 \equiv a \bmod m$.
- The multiplicative inverse exists only for some, but not for all, elements. Let

a ∈ Z, the inverse a^{-1} is defined such that $a \cdot a^{-1} \equiv 1 \bmod m$. If an inverse exists for a, we can divide by this element since $b/a \equiv b \cdot a^{-1} \bmod m$. Finding the inverse is difficult, usually employing the Euclidean algorithm []. An easier method is as follows. An element a ∈ Z has a multiplicative inverse a^{-1} if and only if GCD (a, m) = 1, where GCD is the greatest common divisor. If this holds, then a and m are relatively prime or coprime.

- The distributive law is followed: $a \times (b + c) = (a \times b) + (a \times c)$ for all a, b, c ∈ Z_m. Thus, the ring Z_m is the set of integers {0, 1, 2, ... , m– 1} in which we can add, subtract, multiply, and sometimes divide.

c) Finite Fields

The concept of a simpler algebraic structure, a group is illustrated.

Definition 4

A group is a set of elements G together with an operation ◦ which combines two elements of G. A group is set with one operation and the corresponding inverse operation. If the operation is called addition, the inverse operation is subtraction; if the operation is multiplication, the inverse operation is division (or multiplication with the inverse element).

A group has the following properties:

- The group operation ◦ is closed. That is, for all a, b, ∈ G, it holds that a ◦ b = c ∈ G.
- The group operation is associative. That is, a ◦ (b ◦ c) = (a ◦ b) ◦ c for all a, b, c ∈ G.
- There is an element 1 ∈ G, called the neutral element (or identity element), such that a ◦ 1 = 1 ◦ a = a for all a ∈ G.
- For each a ∈ G there exists an element a^{-1} ∈ G, called the inverse of a, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.
- A group G is abelian (or commutative) if, furthermore, a ◦ b = b ◦ a for all a, b ∈ G.

Cryptography uses both multiplicative groups, i.e., the multiplication, and additive groups. Consider the set of integers $Z_m = \{0, 1, ... , m-1\}$ and the operation addition modulo m. Every element a has an inverse–a such that $a + (-a) = 0 \bmod m$. However, this set does not form a group with the multiplication operation because most elements do not have an inverse where a $a^{-1} = 1 \bmod m$.

Theorem 1

The set Z_n^* which consists of all integers a = 0, 1, ... , n– 1 for which GCD (a, n)= 1 forms an abelian group under multiplication modulo n. The identity element is e = 1. In Table 1 n = 9, so Z_n^* consists of the elements {1, 2, 4, 5, 7, 8}.

Table 1 : Multiplication table for Z_9^*

× mod 9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

The following properties are satisfied:

- Closure: integers which are elements of Z_9^* are used.
- Group identity and inverses: each row and column is a permutation of the elements of Z_9^*.
- Commutativity: symmetry along the main diagonal.
- Associativity: Multiplication in Z_9^*.

In order to have all four basic arithmetic operations (i.e., addition, subtraction, multiplication, division) in one structure, a set which contains an additive and a multiplicative group is needed. This is called a field. A *finite field*, sometimes also called *Galois field*, is a set with a finite number of elements.

Definition 5

A field F is a set of elements with the following properties:

- All elements of F form an additive group with the group operation "+" and the neutral element 0.
- All elements of F except 0 form a multiplicative group with the group operation "×" and the neutral element 1.
- When the two group operations are mixed, the distributive law holds, i.e., for all a, b, c ∈ F: a(b + c)= (ab)+ (ac).

The set R of real numbers is a field with the neutral element 0 for the additive group and the neutral element 1 for the multiplicative group. Thus every real number a has an additive inverse, namely –a, and every nonzero element *a* has a multiplicative inverse 1/*a*. Also note that the number of elements in the field is called the

order or *cardinality* of the field. The following theorem explains the characteristic of a finite field:

Theorem 2

A field with order r only exists if r is a prime power, i.e., $r = c^n$, for some positive integer n and prime integer c. c is called the characteristic of the finite field.

This theorem implies that there are, for instance, finite fields with 243 elements (since $243 = 3^5$) or with 1024 elements (since $1024 = 2^{10}$, and 2 is a prime). However, there is no finite field with 24 elements since $24 = 2^3 \cdot 3$. Hence 24 is thus not a prime power.

The most native examples of finite fields are fields of prime order, i.e., fields with $n = 1$. Elements of the field $GF(c)$ can be represented by integers $0, 1, \ldots, c-1$. The two operations of the field are modular integer addition and integer multiplication modulo c.

Theorem 3

Let c be a prime. The integer ring Z_c^* is denoted as GF(c) and is referred to as a prime field, or as a Galois field with a prime number of elements. All nonzero elements of GF(c) have an inverse. Arithmetic in GF(c) is done modulo c.

This means that the integer ring Z_m^* with modular addition and multiplication, and m happens to be a prime, Z_m^* is not only a ring but also a finite field. In order to do arithmetic in a prime field, the rules for integer rings hold: Addition and multiplication are done modulo c, the additive inverse of any element a is given by $a + (-a) = 0 \bmod c$, and the multiplicative inverse of any nonzero element a is defined as $a \cdot a^{-1} = 1$.

d) Cyclic Groups

Definition of a finite group:

Definition 6

A group (G, ◦) is finite if it has a finite number of elements. We denote the cardinality or order of the group G by $|G|$.

The following are some examples of finite groups:

- $(Z_n^*, +)$: the cardinality of Z_n^* is $|Z_n^*| = n$ since $Z_n^* = \{0, 1, 2, \ldots, n-1\}$.
- $(Z_n^*, \cdot)$: remember that Z_n^* is defined as the set of positive integers smaller than n which are relatively prime to n. Thus, the cardinality of Z_n^* equals Euler's phi function [] evaluated for n, i.e., $|Z_n^*| = \Phi(n)$. For instance, the group Z_9^* has a cardinality of $\Phi(9) = 32 - 31 = 6$. Thus the group consists of the six elements {1, 2, 4, 5, 7, 8}.

Cyclic groups are the basis for discrete logarithm-based cryptosystems. The order of an element is defined as follows:

Definition 7

The order ord(b) of an element b of a group (G, ◦) is the smallest positive integer n such that: $b^n = b \circ b \circ \ldots \circ b = 1$, occurs n times and 1 is the identity element of G.

By using Definition 6, determine the order of $b = 4$ in the group Z_7^*. To do this, compute the powers of b until we obtain the identity element 1.

$$b^1 = b^1 \cdot b^0 = 4 \cdot 1 = 4 \equiv 4 \bmod 7$$
$$b^2 = b^1 \cdot b^1 = 4 \cdot 4 = 16 \equiv 2 \bmod 7$$
$$b^3 = b^2 \cdot b^1 = 2 \cdot 4 = 8 \equiv 1 \bmod 7$$

Shown from the last line: ord(4) = 3. Keep multiplying the result by *b*:

$$b^4 = b^3 \cdot b^1 = 1 \cdot 4 = 4 \equiv 4 \bmod 7$$
$$b^5 = b^4 \cdot b^1 = 4 \cdot 4 = 16 \equiv 2 \bmod 7$$
$$b^6 = b^3 \cdot b^3 = 1 \cdot 1 = 1 \equiv 1 \bmod 7$$

$$b^7 = b^3 \cdot b^4 = 1 \cdot 4 = 4 \equiv 4 \bmod 7$$
$$b^8 = b^3 \cdot b^5 = 1 \cdot 2 = 2 \equiv 2 \bmod 7$$
$$b^9 = b^3 \cdot b^6 = 1 \cdot 1 = 1 \equiv 1 \bmod 7$$

$$b^{10} = b^3 \cdot b^7 = 1 \cdot 4 = 4 \equiv 4 \bmod 7$$
$$b^{11} = b^3 \cdot b^8 = 1 \cdot 2 = 2 \equiv 2 \bmod 7$$
$$b^{12} = b^3 \cdot b^9 = 1 \cdot 1 = 1 \equiv 1 \bmod 7$$

The powers of b run through the sequence {1, 4, 2} indefinitely. This implies that $b = 4$ is a primitive element and $|Z_7^*|$ is cyclic. It follows that ord(b)= 4 = $|Z_7^*|$. The group Z_7^* has the element 4 as a generator.

This cyclic behavior gives rise to following definition:

Definition 8

A group G which contains an element c with maximum order ord(c) = $|G|$ is said to be cyclic. Elements with maximum order are called primitive elements or generators.

An element c of a group *G* with maximum order is called a generator since every element *b* of *G* can be written as a power $c^n = b$ of this element for some *n*, i.e., c *generates* the entire group.

The theorem below states that the multiplicative group of every prime field is cyclic. Thus these groups are the most useful for building discrete logarithm (DL) cryptosystems.

Theorem 4

For every prime p, $(Z_p^*, \cdot)$ is an abelian finite cyclic group.

Theorem 5 first shows Fermat's Little Theorem for all cyclic groups. Secondly it shows that only element orders which divide the group cardinality exist in a cyclic group.

Theorem 5

Let G be a finite group. Then for every a ∈ G it holds that:

- $a|G| = 1$
- ord(a) divides $|G|$

e) Subgroups

Subgroups are subsets of cyclic groups which are groups themselves.

Theorem 6

Let (G, ◦) be a cyclic group. Then every element b ∈ G with ord(s) = t is the primitive element of a cyclic subgroup with t elements.

Consider a subgroup of G $= Z_{11}^*$. Now ord(3) = 5, and the powers of 3 generate the subset J = {1, 3, 4, 5, 9}. To verify whether this set is actually a group its multiplication table has to be explored:

Table 1 : Multiplication table for the subgroup J = {1, 3, 4, 5, 9}

× mod 11	**1**	**3**	**4**	**5**	**9**
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

J is a subgroup of Z_{11}^**:*

- J is closed under multiplication modulo 11 since the table only consists of integers which are elements of J.
- The group operation is obviously associative and commutative since it follows regular multiplication rules.
- The neutral element is 1.
- For every element b ∈ J there exists an inverse b−1 ∈ J which is also an element of J. Every row and every column of the table contain the identity element.
- J is a subgroup of prime order 5.
- The elements 3, 4, 5 and 9 are generators of J.
- Each element b ∈ G of a group G generates some subgroup J.

Subgroups of prime order are of enormous interest in cryptography. The following theorem follows.

Theorem 7

Let J be a subgroup of G. Then |J| divides |G|. Thus the cyclic group Z_{11}^* has cardinality $|Z_{11}^*| = 10 = 1 \cdot 2 \cdot 5$.

Thus, it follows that the subgroups of Z_{11}^* have cardinalities 1, 2, 5 and 10 since these are all possible divisors of 10. All subgroups J of Z_{11}^* and their generators g are given below.

Subgroup	Elements	Primitive Elements
H_1	{1}	g = 1
H_2	{1, 10}	g = 10
H_3	{1, 3, 4, 5, 9}	g = 3, 4, 5, 9

The following theorem gives us immediately a construction method for a subgroup from a given finite cyclic group. The only thing we need is a primitive element and the group cardinality c. One can now simple compute $g^{c/n}$ and obtains a generator of the subgroup with n elements.

Theorem 8

Let G be a finite cyclic group of order c and let g be a generator of G. Then for every integer n that divides c there exists exactly one cyclic subgroup J of G of order n. This subgroup is generated by $g^{c/n}$. J consists exactly of the elements b ∈ G which satisfy the condition $b^n = 1$. There are no other subgroups.

Consider the cyclic group Z_{11}^*. Now g = 8 is a primitive element in the group. To get a generator g for the subgroup of order 2 compute: $q = g^{c/n} = 8^{10/2} = 8^5 = 32768 \equiv 10 \bmod 11$. The element 10 generates the subgroup with two elements:

$$q^1 = 10,$$
$$q^2 = 100 \equiv 1 \bmod 11,$$
$$q^3 \equiv 10 \bmod 11 \ldots$$

f) The Discrete Logarithm in Prime Fields

The discrete logarithm problem (DLP), can directly be explained using cyclic groups. Two important areas are the DLP over Prime fields and the generalized DLP problem. Consider the DLP over Z_p^*, where p is a prime.

Definition 9

Given is the finite cyclic group Z_{11}^* of order p − 1 and a primitive element g ∈ Z_{11}^* and another element q ∈ Z_{11}^*. The DLP is the problem of determining the integer $1 \le x \le p - 1$ such that: $g^x \equiv q \bmod p$.

Such an integer x must exist since g is a primitive element and each group element can be expressed as a power of any primitive element. This integer x is called the discrete logarithm of q to the base g, and we can formally write: $x = \log_g q \bmod p$. Computing discrete logarithms modulo a prime is a very hard problem if the parameters are sufficiently large. Since exponentiation $g^x \equiv q \bmod p$ is computationally easy, this forms a one-way function.

Consider the group Z_{47}^* which has order 46. The subgroups in Z_{11}^* have thus a cardinality of 23, 2 and 1. Now g = 2 is an element in the subgroup with 23 elements, and since 23 is a prime, g = 2 is a primitive element in the subgroup. A possible discrete logarithm problem is given for q = 36 (which is also in the subgroup): Find the positive integer x, $1 \le x \le 23$, such that $2^x \equiv 36 \bmod 47$. By using a brute-force attack, a solution is x = 17.

g) The Generalized Discrete Logarithm Problem

The generalized discrete logarithm problem (GDLP) is used in cryptography and is not restricted to the multiplicative group Z_p^*, p prime, but can be defined over any cyclic groups.

Definition 10

Given is a finite cyclic group G with the group operation ◦ and cardinality k. We consider a primitive

element g ∈ G and another element q ∈ G. The discrete logarithm problem is finding the integer n, where 1≤ n ≤ k, such that: $q = g \circ g \circ \ldots \circ g = g^n$, n times.

Such an integer n must exist since g is a primitive element as in the case of the DLP in Z_p^*. Thus each element of the group G can be generated by repeated application of the group operation on g. Consider the additive group of integers modulo a prime. For instance, choose the prime p = 11, G = (Z_{11}^*, +) is a finite cyclic group with the primitive element g = 2. Here is how g generates the group:

We try now to solve the DLP for the element q = 3, i.e., we have to compute the integer 1≤ n ≤ 11 such that: $n \cdot 2 = 2 + 2 + \ldots + 2$ (n times) ≡ 3 mod 11. Even though the group operation is addition, we can express the relationship between g, q and the discrete logarithm n in terms of multiplication: n· 2 ≡ 3 mod 11. In order to solve for n, invert the primitive element g: n ≡ 2^{-1} 3 mod 11. Using, e.g., the extended Euclidean algorithm, compute 2^{-1} ≡ 6 mod 11 to get the discrete logarithm: n ≡ 2^{-1} 3 ≡ 7 mod 11.

The DLP can be solved easily here as there are mathematical operations which are not in the additive group. They are multiplication and inversion. However, often it was found that the underlying DL problem is not difficult enough.

IV. Elliptic Curve Theory

a) Basic Properties

ECC is based on the generalized discrete logarithm problem. A cyclic group where the DL problem is computationally hard is required. This means that it must have good one-way properties. Polynomials functions with sums of exponents of x and y can be chosen. For example, the polynomial equation $a \cdot x^2 + b \cdot y^2 = c$ over the real numbers turns out to be an ellipse.

An elliptic curve is a special type of polynomial equation. In ECC the curve is not over the real numbers but over a finite field. The most popular choice is prime fields GF(p), where all arithmetic is performed modulo a prime p. The curve is nonsingular so that it has no self-intersections or vertices, and is achieved if the discriminant of the curve $-16*(4a^3 + 27b^2)$ is nonzero.

Definition 11

The elliptic curve over Z_p^*, p > 3, is the set of all pairs (x, y) ∈ Z_p^* which fulfill $y^2 \equiv x^3 + a \cdot x + b$ mod p together with an imaginary point of infinity O, where a, b ∈ Z_p^* and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0$ mod p.

b) Group Operations on Elliptic Curves

"Addition" means that given two points and their coordinates, say A = (x_1, y_1) and B = (x_2, y_2), we have to compute the coordinates of a third point C such that: $A + B = C$ *or* $(x1, y1) + (x2, y2) = (x3, y3)$. Two cases are considered:

- the addition of two distinct points (point addition)
- the addition of one point to itself (point doubling)

Point Addition P + Q : This is the case where we compute R = P + Q and P ≠ Q. The construction works as follows: A line through P and Q intersects a third point between the elliptic curve and the line. Mirror this third intersection point along the x-axis. This mirrored point is, by definition, the point R. Figure 1 shows the point addition on an elliptic curve over the real numbers.

i	1	2	3	4	5	6	7	8	9	10	11
ig	2	4	6	8	10	1	3	5	7	9	0

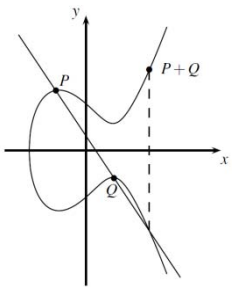


Figure 1 : Point addition on an elliptic curve over the real numbers

Point Doubling P + Q : This is the case where we compute P + Q but P = Q. Hence, R = P + P = 2P. First draw the tangent line through P and obtain a second point of intersection between this line and the elliptic curve. Then mirror the second point of intersection along the x-axis. This mirrored point is the result R of the doubling as shown in Figure 2.

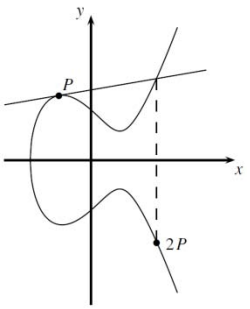


Figure 2 : Point doubling on an elliptic curve over the real numbers

With these operations the points on the elliptic curve fulfill the group conditions: closure, associativity, existence of an identity element and existence of an inverse. Consider the add, subtract, multiply and divide operations over prime fields GF(p) rather than over the real numbers. The following analytical expressions become relevant. The elliptic curve point addition and doubling formulae are shown:

if P ≠ Q (point addition), $s = \frac{y_2 - y_1}{x_2 - x_1} \ mod \ p$

if P = Q (point doubling), $s = \frac{3x_1^2 + a}{2y_1} \ mod \ p$

then

$x_3 = s^2 - x_1 - x_2 \ \text{mod} \ p$

$y_3 = s*(x_1 - x_3) - y_1 \bmod p$

The parameter s is the slope of the line through P and Q in the case of point addition, or the slope of the tangent through P in the case of point doubling. An identity (or neutral) element O such that: $P + O = P$ is compulsory. An abstract point at infinity is used as the neutral element O. This point at infinity is located towards "plus" infinity along the y-axis or towards "minus" infinity along the y-axis. Hence, the inverse $-P$ of any group element P is: $P + (-P) = O$.

- Finding the inverse of a point $P = (x_p, y_p)$ is the negative of its y coordinate. In the case of elliptic curves over a prime field GF(p) as $-y_p \equiv p - y_p \bmod p$, hence $-P = (x_p, p - y_p)$. An example for the group operation is now given. Consider a curve over the small field Z_{29}^*, $E : y^2 \equiv x^3 + 2x + 2 \bmod 17$. To double the point $A = (3, 1)$:

- $2P = P + P = (3, 1) + (3, 1) = (x_3, y_3)$.
- Now $s = (2 \cdot 1) - 1 * (3 \cdot 32 + 2) = 2 - 1 \cdot 29 \equiv 9 \cdot 12 = 63 \equiv 6 \bmod 1$.
- Also $x3 = s2 - x1 - x2 = 62 - 3 - 3 = 30 \equiv 13 \bmod 17$.
- And $y3 = s(x1 - x3) - y1 = 6 * (3 - 13) - 1 = -61 \equiv 7 \bmod 17$.
- Thus, $2P = (3, 1) + (3, 1) = (13, 7)$.

Inserting the coordinates into the curve equation: $y^2 \equiv x^3 + 2 \cdot x + 2 \bmod 17 = 7^2 \equiv 13^3 + 2 \cdot 13 + 2 \bmod 17$. So $15 = 2225 \equiv 15 \bmod 17$ which proves that the point is actually on the curve.

c) Building a Discrete Logarithm Problem with Elliptic Curves

Setting up the discrete logarithm problem is now discussed.

Definition 12

Given an elliptic curve E, consider a primitive element P and another element R. The DL problem is finding the integer d, where $1 \le d \le \#E$, such that: $P + P + \cdots + P = d * P = U$. P is repeated d times. In cryptosystems, d is the private key which is an integer, while the public key U is a point on the curve with coordinates $U = (x_u, y_u)$.

The operation in Definition 12 is called point multiplication. Thus, formally $U = d * P$. Note d*P is a notation for this repeated group operation. If a multiplicative notation is chosen, the ECDLP would have had the form $P^d = U$, which would have been more consistent with the conventional DL problem in Z_{29}^*.

Given a starting point P for the ECDLP elliptic curves over the real numbers, the computation becomes 2P, 3P, .. ., d*P = U . This is effectively hopping back and forth on the elliptic curve. The starting point P (a public parameter) and the final point U (the public key) is put in the public domain. To break the cryptosystem, an attacker has to figure out how often we "jumped" on the elliptic curve. Thus, the number of hops is the secret d, the private key.

V. Elliptic Curve Cryptosystems

a) Elliptic Curve Diffie–Hellman

As with the conventional Diffie–Hellman key exchange (DHKE) [] a key exchange using elliptic curves can be realized. This elliptic curve Diffie–Hellman key exchange (ECDH) requires agreed upon domain parameters on an elliptic curve and a primitive element on this curve:

- Choose a prime p and the elliptic curve: $E : y^2 \equiv x^3 + a \cdot x + b \bmod p$
- Choose a primitive element $P = (x_P, y_P)$. The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters.

The actual key exchange is the same as for the conventional Diffie–Hellman protocol. Alice and Bob choose the private keys a and b, respectively, which are two large integers. With the private keys both generate their respective public keys A and B, which are points on the curve. The public keys are computed by point multiplication. The two parties exchange these public parameters with each other. The joint secret T_{AB} is then computed by both Alice and Bob by performing a second point multiplication involving the public key they received and their own secret parameter. The joint secret T_{AB} can be used to derive a session key, e.g., as input for the AES algorithm []. Note that the two coordinates (x_{AB}, y_{AB}) are not independent of each other: Given x_{AB}, the other coordinate can be computed by simply inserting the x value in the elliptic curve equation.

Thus, only one of the two coordinates should be used for the derivation of a session key. EC-DH Key Exchange is now shown.

Alice	**Bob**
choose k_{prA} $= a \in \{2, 3, ..., \#E - 1\}$	choose k_{prB} $= b \in \{2, 3, ..., \#E - 1\}$
compute k_{pubA} $= a*P = A = (x_A, y_A)$	compute k_{pubB} $= b*P = B = (x_B, y_B)$
$A = (x_A, y_A)$ →	
← $B = (x_B, y_B)$	
compute $a_B = T_{AB}$	compute $b_A = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

Proof. Alice computes aB = a (b P) while Bob computes bA = b (a P). Since point addition is associative, both parties compute the same result, namely the point $T_{AB} = ab\ P$.

Let's look at an example with small numbers.

We consider the ECDH with the following domain parameters. The elliptic curve is $y^2 \equiv x^3 + 2x + 2 \bmod 17$, which forms a cyclic group of order $\#E = 19$. The base point is $P = (5, 1)$. The protocol proceeds as follows:

Alice	**Bob**
choose $k_{prA} = a = 3$	choose $k_{prB} = b = 10$
compute k_{pubA} $= a^* P$ $= 3P$ $= (10, 6) = A$	compute k_{pubB} $= b^* P$ $= 10P$ $= (7, 11) = B$
$A = (10, 6)$ →	
← $B = (7, 11)$	
compute a*B $= T_{AB}$ $= 3(7, 11)$ $= (13, 10)$	compute b*A $= T_{AB}$ $= 10(10, 6)$ $= (13, 10)$

Joint secret between Alice and Bob: $T_{AB} = (13, 10)$.

b) The Elliptic Curve Digital Signature Algorithm (ECDSA)

The ECDSA standard is defined for elliptic curves over prime fields Z_p and Galois fields $GF(2^m)$. The former is often preferred in practice, and is used in what follows. The keys for the ECDSA are computed as follows:

i. *Key Generation for ECDSA*

Use an elliptic curve E with modulus p, coefficients a and b and a point A which generates a cyclic group of prime order q. Then choose a random integer d with $0 < d < q$. Finally compute $B = d A$. The keys are now: $k_{pub} = (p, a, b, q, A, B)$ and $k_{pr} = (d)$.

Note that we have set up a discrete logarithm problem where the integer d is the private key and the result of the scalar multiplication, point B, is the public key. Similar to DSA, the cyclic group has an order q which should have a size of at least 160 bit or more for higher security levels.

ii. *Signature and Verification*

The ECDSA signature consists of a pair of integers (r, s). Each value has the same bit length as q, which makes for fairly compact signatures. Using the public and private key, the signature for a message x is computed as follows.

iii. *ECDSA Signature Generation*

- Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
- Compute $R = k_E A$.
- Let $r = x_R$.

Compute $s \equiv (h(x) + d \cdot r)\, k_E^{-1} \bmod q$

In step 3 the x-coordinate of the point R is assigned to the variable r. The message x has to be hashed using the function h in order to compute s. The hash function output length must be at least as long as q. The hash function compresses x and computes a fingerprint which can be viewed as a representative of x. The signature verification process is as follows.

iv. *ECDSA Signature Verification*

- Compute auxiliary value $w \equiv s^{-1} \bmod q$.
- Compute auxiliary value $u_1 \equiv w \cdot h(x) \bmod q$.
- Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
- Compute $P = u_1 A + u_2 B$.

The verification $ver_{k_{pub}}(x, (r, s))$ follows from: $x_P \equiv r \bmod q \Rightarrow$ valid signature and $x_P \not\equiv r \bmod q \Rightarrow$ invalid signature.

In the last step, the notation x_P indicates the x-coordinate of the point P. The verifier accepts a signature (r, s) only if the x_P has the same value as the signature parameter r modulo q. Otherwise, the signature should be considered invalid.

Proof. We show that a signature (r, s) satisfies the verification condition $r \equiv x_P \bmod q$.

We'll start with the signature parameter s.

$s \equiv (h(x) + d\, r)\, k_E^{-1} \bmod q$

$= k_E \equiv s^{-1} h(x) + d\, s^{-1} r \bmod q$

Use the auxiliary values u_1 and u_2:

$= k_E \equiv u_1 + d\, u_2 \bmod q$

Multiply both sides of the equation with A as the point A generates a cyclic group of order q:

$= k_E A = (u_1 + d\, u_2) A$

Group operation is associative:

$= k_E A = u_1 A + d\, u_2 A$

Group operation is associative:

$= k_E A = u_1 A + u_2 B$

Thus the expression $u_1 A + u_2 B$ is equal to $k_E A$ if the correct signature and key (and message) have been used. But this is exactly the condition that we check in the verification process by comparing the x-coordinates of $P = u_1 A + u_2 B$ and $R = k_E A$.

Bob wants to send a message to Alice that is to be signed with the ECDSA algorithm. The signature and verification process is as follows. The elliptic curve E: $y^2 \equiv x^3 + 2x + 2 \bmod 17$. All points of the curve form a cyclic group of order 19, i.e., a prime, there are no subgroups and hence in this case $q = \#E = 19$.

Alice	**Bob**
	choose E with p = 17, a =2, b = 2, and A = (5, 1). with q = 19, choose d = 7. Compute B = d A = 7 (5, 1) = (0, 6)
	← (p, a, b, q, A, B)
	(17, 2, 2, 19, (5, 1), (0, 6))
	sign: compute hash of message h(x) = 26 choose ephemeral key k*E = 10

$R = 10\,(5, 1) = (7, 11)$

$r = x*R = 7$

$s = (26 + 7 \,.\, 7) \,.\, 2 \equiv 17 \bmod 1$

$(x, (r, s)) = (x, (7, 17))$ ←

verify:

$w = 17^{-1} \equiv 9 \bmod 19$

$u_1 = 9 \cdot 26 \equiv 6 \bmod 19$

$u_2 = 9 \cdot 7 \equiv 6 \bmod 19$

$P = 6 \cdot (5, 1) + 6 \cdot (0, 6) = (7, 11)$

$x_P \equiv r \bmod 19 \Rightarrow$ valid signature

c) Elliptic Curve Integrated Encryption Scheme (ECIES)

Elliptic curve cryptography can be used to encrypt plaintext messages, M, into ciphertexts. The elliptic group $E_p(a, b)$ and the generator point G are made public. Each user select a private key, $n_A < n$ and compute the public key P_A as: $P_A = n_A*G$. To encrypt the message point P_M for Bob (B), Alice (A) choses a random integer k and compute the ciphertext pair of points P_C using Bob's public key P_B:

$$P_C = [(k*G),(P_M + k*P_B)]$$

After receiving the ciphertext pair of points, P_C, Bob multiplies thefirst point, (k*G) with his private key, n_B, and then adds the result to the second point in the ciphertext pair of points, $(P_M + k*P_B)$:

$$(P_M + k*P_B) - [n_B(k*G)] = (P_M + k*n_BG) - [n_B(k*G)] = P_M$$

which is the plaintext point, corresponding to the plaintext message M. Only Bob, knowing the private key n_B, can remove $n_B(k*G)$ from the second point of the ciphertext pair of point, i.e. $(P_M + k*P_B)$, and hence retrieve the plaintext information P_M.

Consider the following elliptic curve: $y^2 = x^3 - x + 188 \bmod 751$ that is: $a = -1$, $b = 188$, and $p = 751$. The elliptic curve group generated by the above elliptic curve is $E_p(a,b) = E_{751}(-1,188)$. Let the generator point $G = (0,376)$. Then the multiples k*G of the generator point G are (for $1 \le k \le 751$):

$G = (0,376)$ $2G = (1,376)$ $3G = (750,375)$ $4G = (2,373)$ $5G = (188,657)$ $6G = (6,390)$ $7G = (667,571)$ $8G = (121,39)$ $9G = (582,736)$ $10G = (57,332)$ ... $761G = (565,312)$ $762G = (328,569)$ $763G = (677,185)$ $764G = (196,681)$ $765G = (417,320)$ $766G = (3,370)$ $767G = (1,377)$ $768G = (0,375)$ $769G = O$ (point at infinity)

If Alice wants to send to Bob the message M which is encoded as the plaintext point $P_M = (443,253) \in E_{751}(-1,188)$. She must use Bob public key to encrypt it. Suppose that Bob secret key is $n_B = 85$, then his public key will be: $P_B = n_B*G = 85(0,376) = (671,558)$. Alice selects a random number $k = 113$ and uses Bob's public key $P_B = (671,558)$ to encrypt the message point into the ciphertext pair of points:

$P_C = [(k*G),(P_M + k*P_B)]$

$= [113 \times (0,376),(443,253) + 113 \times (671,558)]$

$= [(34,633),(443,253) + (47,416)]$

$= [(34,633),(217,606)]$

Upon receiving the ciphertext pair of points, $P_C = [(34,633), (217,606)]$, Bob uses his private key, $n_B = 85$, to compute the plaintext point, P_M, as follows.

$(P_M + k*P_B) - [n_B(k*G)] = (217,606) - [85(34,633)]$

$= (217,606) - [(47,416)]$

$= (217,606) + [(47,-416)]$ (since $-P = (x_1, -y_1)$)

$= (217,606) + [(47,335)]$ (since $-416 \equiv 335 \bmod 751$)

$= (443,253)$

and then maps the plaintext point $P_M = (443,253)$ back into the original plaintext message M.

VI. Security of ecc Cryptosystems

a) Security of EC-DH

Elliptic curves are used as the ECDLP has very good one-way characteristics. E, p, P, A, and B is available for an attacker who wants to break the ECDH. The attacker desires to compute the joint secret between Alice and Bob $T_{AB} = a * b * P$. This is known as the elliptic curve Diffie–Hellman problem (ECDHP). Presently, there seems to be only one way to compute T_{AB}, that is, to solve either $a = \log_P A$, or $b = \log_P B$. Each of which are discrete logarithm problems.

For carefully chosen elliptic curve the best known attacks against the ECDLP are considerably weaker than the best algorithms for solving the DL problem modulo p, and the best factoring algorithms which are used for RSA attacks. In particular, the index-calculus algorithms [22], which are powerful attacks against the DLP modulo p, are not applicable against elliptic curves. For carefully selected elliptic curves, the only remaining attacks are generic DL algorithms, that is, Shanks' baby-step giant-step method [19] and Pollard's rho method [1].

As the number of steps required for such an attack is approximately equal to the square root of the group cardinality, a group order of at least 2^{160} should be used. An attack with a group consisting of generic algorithms, will require about 2^{80} steps. Thus, a security level of 80 bits provide moderate security. Thus, in practice elliptic curve bit lengths of up to 256 bits are commonly used. This will provide security levels of up to 128 bits.

b) Security of ECDSA

Elliptic curves have several advantages over RSA and over DL schemes like Elgamal or DSA. In particular, the absence of strong attacks against elliptic curve cryptosystems (ECC), bit lengths in the range of 160–256 bit can be chosen which provide security equivalent to 1024–3072-bit RSA and DL schemes. The shorter bit length of ECC often results in shorter processing time and in shorter signatures.

Given that the elliptic curve parameters are chosen correctly, the main analytical attack against ECDSA attempts to solve the elliptic curve discrete logarithm problem. If an attacker were capable of doing this, he could compute the private key d and/or the ephemeral key. However, the best known ECC attacks have a complexity proportional to the square root of the size of the group in which the DL problem is defined, i.e., proportional to $\sqrt{q}$.

The security level of the hash function must also match that of the discrete logarithm problem. The cryptographic strength of a hash function is mainly determined by the length of its output. The security levels of 128, 192 and 256 were chosen so that they match the security offered by AES with its three respective key sizes. More subtle attacks against ECDSA are also possible. For instance, at the beginning of verification it must be checked whether r, s $\in$ {1, 2,..., q}. Also, protocol-based weaknesses, e.g., reusing the ephemeral key, must be prevented.

c) Security of ECIES

The cryptographic strength of elliptic curve encryption lies in the difficulty for a cryptanalyst to determine the secret random number k from k*P and P itself. The fastest method to solve this problem (known as the elliptic curve logarithm problem) is the Pollard ρ factorization method [].

The computational complexity for breaking the elliptic curve cryptosystem, using the Pollard ρ method, is 3.8×1010 MIPS-years (i.e. millions of instructions per second times the required number of years) for an elliptic curve key size of only 150 bits []. Finally increasing the elliptic curve key length to only 234 bits will impose a computational complexity of 1.6 × 1028 MIPS-years (still with the Pollard ρ method).

VII. Conclusion

Public-key encryption can be used to eliminate problems involved with conventional encryption. However, it has not managed to be as widely accepted as conventional encryption because it introduces a lot of overheads. Therefore, it is very important to find ways to reduce the overheads yet not sacrificing on other aspects of security so that the desirability in public-key can be exploited.

ECC have been described, which is a promising candidate for the next generation public-key cryptosystem. Although ECC's security has not been completely evaluated, it is expected to come into widespread use in various fields in the future.

ECC has been shown to have many advantages due to its ability to provide the same level of security as other public key cryptosystems, yet using shorter keys. However, its disadvantage which may even hide its attractiveness is its lack of maturity, as mathematicians believed that enough research has not yet been done in ECDLP. Finally, the future of ECC looks brighter than that of other public key cryptosystems as today's applications (smart cards, pagers, and cellular telephones etc) cannot afford the associated overheads.

References Références Referencias

1. Bach, E. (1991). Toward a theory of Pollard's rho method. Information and Computation, 90(2), 139-155.
2. Banavar, G., & Bernstein, A. (2002). Software infrastructure and design challenges for ubiquitous computing applications. *Communications of the ACM*, *45*(12), 92-96.
3. Brent, R. P. (2010). Some integer factorization algorithms using elliptic curves. *arXiv preprint arXiv:1004.3366*.
4. Davis, V. M., Cutino, S. C., Berg, M. J., Conklin, F. S., & Pringle, S. J. (2001). U.S. Patent No. 6,282,522. Washington, DC: U.S. Patent and Trademark Office.
5. Denning D. E. R., Denning P. J. Internet besieged: Countering cyberspace scofflaws. ACM Press, 1998.
6. ElGamal, T. (1985, January). A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology (pp. 10-18). Springer Berlin Heidelberg.
7. Ferri, R., Kim, M., & Yee, E. (2004). U.S. Patent Application 10/856,684.
8. Finkenzeller, K. (1999). RFID handbook: radio-frequency identification fundamentals and applications (pp. 151-158). New York: Wiley.
9. Gordon, D. (2011). Discrete logarithm problem. In Encyclopedia of Cryptography and Security (pp. 352-353). Springer US.
10. Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1(1), 36-63.
11. Kanayama, N., Kobayashi, T., Saito, T., & Uchiyama, S. (2000). Remarks on elliptic curve discrete logarithm problems. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *83*(1), 17-23.
12. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.
13. Lahiri, S. (2005). RFID sourcebook. IBM press.
14. McLoone, M., & Robshaw, M. J. (2006). Public key cryptography and RFID tags. In Topics in Cryptology–CT-RSA 2007 (pp. 372-384). Springer Berlin Heidelberg.
15. Messer, A., Greenberg, I., Bernadat, P., Milojicic, D., Chen, D., Giuli, T. J., & Gu, X. (2002). Towards a distributed platform for resource-constrained devices. In Distributed Computing Systems, 2002.

Proceedings. 22nd International Conference on (pp. 43-51). IEEE.

16. Miller, V. S. (1986, January). Use of elliptic curves in cryptography. In Advances in Cryptology—CRYPTO'85 Proceedings (pp. 417-426). Springer Berlin Heidelberg.
17. Montgomery, P. L. (1994). A survey of modern integer factorization algorithms. CWI quarterly, 7(4), 337-366.
18. Peralta, R. (1986, January). Simultaneous security of bits in the discrete log. In *Advances in Cryptology—Eurocrypt'85* (pp. 62-72). Springer Berlin Heidelberg.
19. Pollard, J. M. (2000). Kangaroos, monopoly and discrete logarithms. Journal of cryptology, 13(4), 437-447.
20. Rankl, W., & Effing, W. (2010). *Smart card handbook*. John Wiley & Sons.
21. Shoup, V. (1995). A new polynomial factorization algorithm and its implementation. Journal of Symbolic Computation, 20(4), 363-397.
22. Silverman, J. H., & Suzuki, J. (1998, January). Elliptic curve discrete logarithms and the index calculus. In Advances in Cryptology—ASIACRYPT'98 (pp. 110-125). Springer Berlin Heidelberg.
23. Smart, N. P. (2001). The exact security of ECIES in the generic group model. In Cryptography and Coding (pp. 73-84). Springer Berlin Heidelberg.
24. Zhao, W., Ramamritham, K., & Stankovic, J. A. (1987). Scheduling tasks with resource requirements in hard real-time systems. *Software Engineering, IEEE Transactions on*, (5), 564-577.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Improving IEEE 802.11 Wlan Handoff Latency by Access Point-based Modification

By Nidhi Sanghavi & Rajesh S. Bansode
Mumbai University, India

Abstract- IEEE 802.11 WLAN provides multimedia services like live telecast, video streaming, video conferencing, Voice over IP (VoIP) to its users. For deployment of these fast real time services, it needs stringent Quality of service (QoS) requirement such as delay time less than 150ms for VoIP, and packet loss rate of 1%. The mobility service for users come with cost of handoff process required when mobile stations get connected from 1 Access point (AP) to another for continuous service. In existing 802.11 IEEE handoff procedure, the scanning phase can exceed duration of 200ms and packet loss can exceed 10%. Thus, proposed methodology focuses on achieving reduced overall handoff latency by implementing handoff delay duration less than 150ms which is the need for seamless service in IEEE 802.11 WLAN.

Keywords: IEEE 802.11 wlan, handoff latency, delay, access point, mish, seamless handoff, ns2.

GJCST-E Classification : C.2.6

Strictly as per the compliance and regulations of:

Improving IEEE 802.11 Wlan Handoff Latency by Access Point-based Modification

Nidhi Sanghavi [α] & Rajesh S. Bansode [σ]

Abstract- **IEEE 802.11 WLAN provides multimedia services like live telecast, video streaming, video conferencing, Voice over IP (VoIP) to its users. For deployment of these fast real time services, it needs stringent Quality of service (QoS) requirement such as delay time less than 150ms for VoIP, and packet loss rate of 1% . The mobility service for users come with cost of handoff process required when mobile stations get connected from 1 Access point (AP) to another for continuous service. In existing 802.11 IEEE handoff procedure, the scanning phase can exceed duration of 200ms and packet loss can exceed 10%. Thus, proposed methodology focuses on achieving reduced overall handoff latency by implementing handoff delay duration less than 150ms which is the need for seamless service in IEEE 802.11 WLAN.**

Keywords: IEEE 802.11 wlan, handoff latency, delay, access point, mish, seamless handoff, ns2.

I. Introduction

The IEEE 802.11 WLAN is widely used for its simple deployment and low cost. There are two operating modes in this network namely, ad-hoc and infrastructure mode. In ad-hoc mode, two or more mobile stations (STA) establish and interact via peer-to-peer communication whereas in infrastructure mode, there is a fixed entity called Access Point (AP). The AP bridges data between the mobile stations (STA) associated to it. The Mobile stations and the associated AP together form a Basic Service set (BSS), also collection of APs extends BSS into Extended Service Set (ESS).

Within IEEE 802.11 wireless Local Area Networks (WLANs), a handoff occurs when a mobile station (STA) moves beyond the radio range of associated AP, and enters another BSS at the MAC layer. Mobile station moves its association from one Access Point to another. Thus, when mobile station changes its APs, it starts a process called as handoff. Now, during this handoff process, the client station is unable to send or receive any data packets. This is called as handoff latency which can exceed the duration of 200 milliseconds. For applications like VoIP, it is required that a delay of less than 150 milliseconds and packet loss less than 3% should persist [1]. Thus there is a need to provide fast handoff solutions to support VoIP services and other multimedia traffic without disruptions to mobile users.

This paper is organized as follows: in Section II, overview of the basic handoff process and related work done is described. In Section III, there is briefing of methodology used. In Section IV, simulation set-up and results are discussed. Finally, paper is concluded in the section V.

II. Background & Related Work

a) Basic Handoff Procedure

The basic handoff procedure is explained in the Fig 1, where a station is connecting to an access point. The probe request, probe response, authentication and re-association messages are communicated between the station and Access Point (AP).

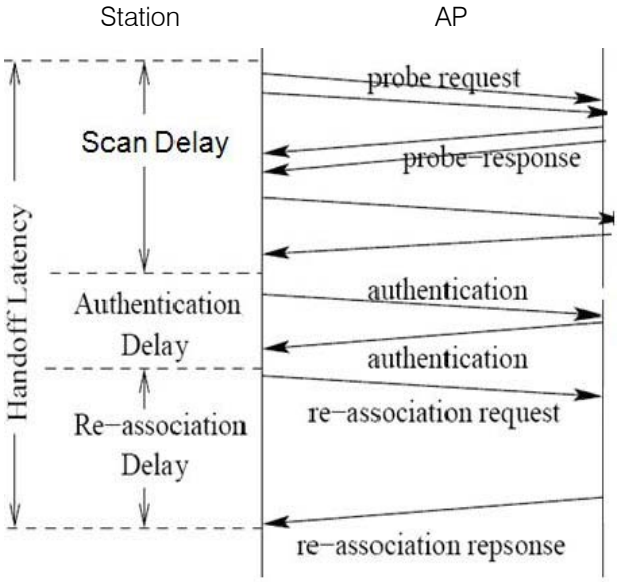


Figure 1 : Basic Handoff Procedure

A handoff occurs when a mobile station moves beyond the radio range of one AP, and enters another BSS at the MAC layer. In this process, there are three entities participating namely moving station, a prior-AP, a posterior-AP [2]. The AP to which station has connectivity prior to handoff process is prior-AP and the new AP to which it associates after handoff process is posterior-AP. The handoff procedure is divided into two phase [3].

Author α : Master of engineering in Information technology, TCET, Mumbai university, India. e-mail: sanghavinidhi23.ns@gmail.com
Author σ : Associate professor in Department of Information technology TCET, Mumbai university, India.
e-mail: rajesh.bansode1977@gmail.com

Phase 1: Discovery process can be active or passive scanning of the neighboring APs which the mobile station can be associated with. Active scanning mobile station sends probe request to APs and waits for probe responses, whereas passive scanning includes waiting for beacon messages sent periodically by AP.

Phase 2: Re-Authentication process, it entails Authentication and Re-association to new AP. There authentication involves transfer of credentials from old-AP to new-AP. Thus, handoff latency is blend of Scan-delay during Discovery phase, and Authentication delay and re-association delay during Re-authentication phase.

b) Related work

The related work is broken into two distinct categories:

1. Modifications inculcated on stations (mobile-nodes) configuration to improve handoff latency.
2. AP-based modification to reduce handoff interruption and duration time and thus improve handoff latency.

To reduce handoff latency many approaches such as, [4]-[6] have been proposed which involve modifications at mobile node. In [4], the author has introduced a concept called as neighbor graph (NG). With help of NG, mobile node has to scan only the current AP's neighbor. In this algorithm, cache size is to be considered while storing the NG on it. Reference [5], a new approach called Synscan is proposed, where clients passively scan all the channels by switching its current channel. There is time synchronization for beacon messages, thus it eliminates the need of AP discovery in handoff procedure. In paper [6], author has used two radios in mobile node, where one radio scans all APs and other keeps communicating with current AP.

Other category, where algorithms propose modification at AP –side are described in references [7]-[9]. In the paper [7] by authors F.Rousseau and Y.Grunenberger proposes the concept of virtual access points to manage mobile station in infrastructure networks. In this scheme, stations are not aware that they move, and all the complexity is pushed back inside the network. It is then possible to control mobility from a global point of view, to optimize network resources for mobile stations, hence providing a better quality of service.

In this paper [8], the authors S.Jin, M.Choi, S.Choi and L.Wang define a scanning scheme composed of two phases : 1.Channel selection phase 2. AP search phase in order to accelerate AP-finding process. In this paper, two algorithms are developed to improve scanning latency i:e near best-fit and first-fit algorithm. Near best-fit algorithm helps the scanning station to find AP providing the highest data rate among neighboring APs. First-fit algorithm enables scanning station stop its scanning when it discovers an AP that satisfies its requirements.

In this paper [9], a novel scanning scheme for IEEE 802.11 by equipping Access Points (APs) with multiple Wireless Network Interface Cards (Multi-WNICs) is proposed, where one is set to operate in an exclusively reserved channel for the scanning purpose. In this environment, a Station (STA) can easily search neighboring APs by scanning the reserved channel.

III. Methodology

The Fig 2 below describes the MISH protocol [10], Multiple –Interface Seamless handoff where Each AP has multiple WNIC (Wireless Network Interface cards) working in different channels

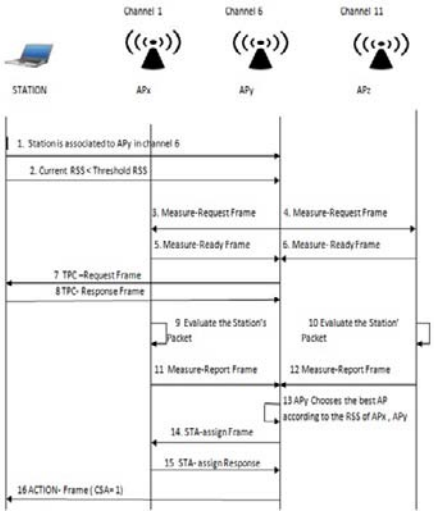


Figure 2 : MISH Protocol

ALGORITHM :

Step 1 : Station is associated to APy in Channel 6

Step 2 : The current RSS of Station's packets < Threshold RSS (thus need for handoff)

Step 3 & 4 : Associated AP i:e APy sends a MEASURE-Request Frame to other neighbor APS

MEASURE-Request Frame MAC address of connected Station

Step 5 & 6 : Neighboring APS send MEASURE-Ready Frame to Associated AP

MEASURE-Ready Frame Confirmation & Ready to receive packets from connected Station

Step 7 : Associated AP, APy sends A TPC-Request Frame to connected Station

TPC-Request Frame Transmit Power control (defined by 802.11h) all 802.11 devices support

Step 8 : Station sends TPC-Response Frame to Channel 6(Associated APy), now this TPC- Response Frame is also received by APx and APz because their 1WNIC is listening on channel 6.

Step 9 & 10 : By receiving TCP-Response Frame from Station, neighboring APs i:e APx & APz measures RSS of packet received from the Station

Step 11 & 12 : Neighboring APs i:e APx and APy send a MEASURE-Report Frame to associated AP (APy)

MEASURE-Report Frame

RSS value of the packet(TPC-Response) received from station

Step 13 : After receiving Measure-Report Frame from neighboring APs, Associated AP chooses the best next AP (according to the value of RSS)
ASSUME APy CHOSE APx

Step 14 : Old AP(APy) sends a STA-Assign Frame to new chosen AP(APx)

STA-Assign Frame

1 .MAC address of station

2. Messages Station's previous authentication and association messages

Step 15 : New chosen AP (APx) sends STA- assign Response Frame to old AP (APy)

STA- assign Response

1. To give confirmation to old AP

2. Assign an Association ID to the Station

Step 16 : Finally. Old AP(APy) sends a ACTION-frame to the station

ACTION-frame

CSA (Channel Switch announcement) here, CSA= 1

(because station has to switch association from channel 6 to channel 1).

To Notify the Station about following changes to be done;

IV. Simulation Set-up & Results

A simulation model using ns2 has been developed to evaluate the methodology mentioned in previous section.

The simulations were performed using Network Simulator 2 (NS-2.34). The traffic sources are Constant Bit Rate (CBR). The source destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' in a rectangular field of 1000m x 1000m with 100 nodes.

The various simulation parameters and the values used are described in the table below

Table 1 : Simulation Parameter List

Simulator	NS2
Simulation area	1000*1000m
MAC Protocol	Modified 802.11(802_11_STA)
Packet size	512 bytes
Simulation Time	200 secs
Traffic Sources	Udp (CBR)
Interval(Pause between movements)	0.05
Radio range	250m
ChannelSwitchDelay	200ms
MaxChannelTime	40ms
MinChannelTime	20ms

The design of simulation includes Grid topology, there are 16 APs(Access Points) and 4 MN(Mobile Nodes) in the simulation area that has been considered. Fig 3 depicts the grip topology .

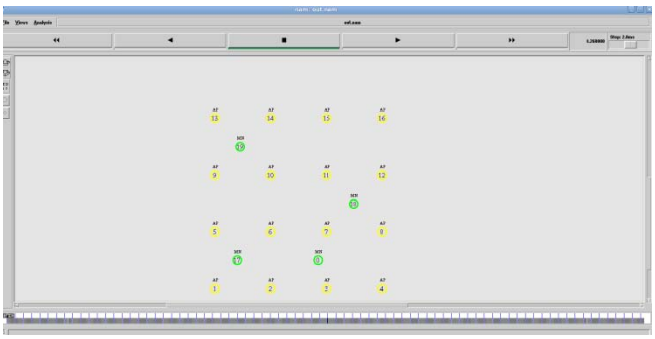


Figure 3 : Grid topology

Fig 4 demonstrates the handoff procedure as the mobile nodes starts their random mobility movement. The circles depict the radio range of each AP in the grid topology in the simulation

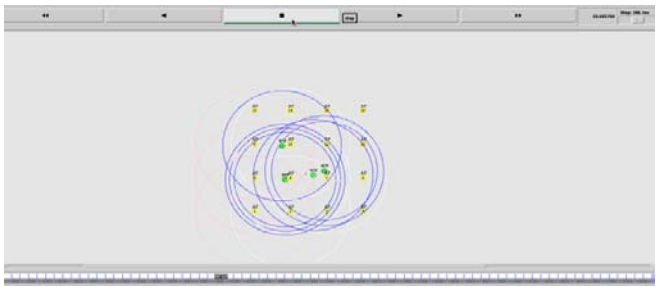


Figure 4 : Handoff simulation as mobile nodes start Moving

The total handoff delay duration for 200sec simulation is 0.0366024 seconds. The MinChannelTime and Max Channel Time is considered as 20ms and 40ms respectively. The ChannelSwitchDelay is 200ms. The handoff Interruption time is 0.022362 seconds Fig 5 shows the graph of interval plotted against handoff Delay. As the time interval between the sending of packets increases, handoff delay duration also gradually increases.

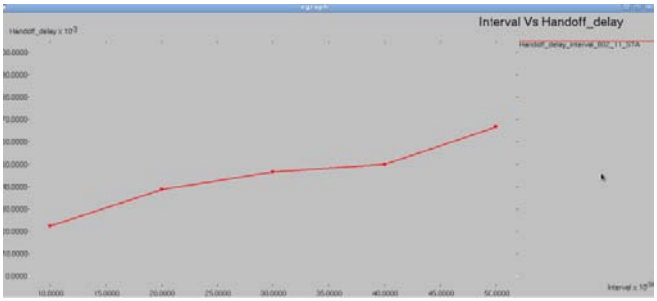


Figure 5 : Handoff delay vs. Interval between packets

Fig 6 depicts a graph that plots handoff delay duration against packetsize of the data packet. As the size of datapacket decreases, the handoff delay duration also decreases.

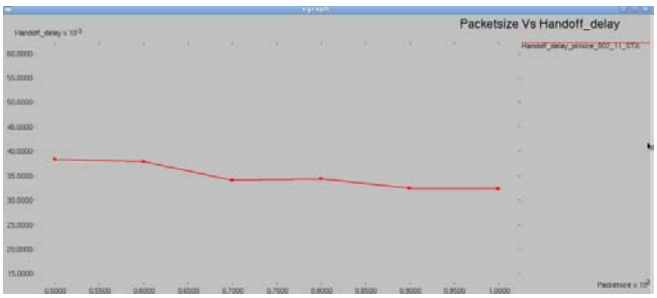


Figure 6 : Handoff delay vs packetsize

V. Conclusion

The mobility management is an important factor IEEE 802.11 provides to the users. For seamless services like video conferencing, VoIP, there is stringent requirement of less than 150ms handoff delay. The legacy handoff protocol provides handoff delay for more than 200ms. Thus there is a need for Seamless handoff protocol that would provide continuous services without interruption to clients in IEEE 802.11 WLAN. Thus the MISH protocol have been successful in meeting this Qos requirements since handoff delay is 36.6024 ms.

References Références Referencias

1. Hongqiang Zhai, Xiang Chen, and Yuguang Fang. "How well can the IEEE 802.11 wireless LAN support quality of service?," IEEE Trans. Wireless Communications, vol. 4, pp.3084–3094, Dec. 2005.
2. A. Mishra, M. Shin, and W. Arbaugh,"An empirical analysis of the IEEE 802.11 MAC layer handoff process,"SIGCOMM Comput. Commun. Rev, vol. 33, no. 2, pp. 93–102, 2003.
3. Y. Pawar and V. Apte, "Improving the IEEE 802.11 MAC Layer Handoff Latency to Support Multimedia Traffic", in IEEE Conference on Wireless Communication and Networking Conference, pp. 1-6, 2009.
4. Minho Shin, Arunesh Mishra, and William A. Arbaugh, " Improving the latency of 802.11 hand-offs using neighbor graphs,"in Proc. MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services, pp. 70-88, ACM, New York, 2004.
5. S. Ramani, I. Savage. (2005)."Syncscan: Practical fast handoff for 802.11 infrastructure networks.", INFOCOM 2005. 24th Annual Joint conference of the IEEE computer & communication societies, Proc. IEEE 1, pp. 675-689, vol 1.
6. A. Mishra V. Brik and S. Banerjee. " Eliminating handoff latencies in 802.11 WLANS using multiple radios: Applications, experience, and evaluation.", ACM IMC, Oct. 2005.
7. S. Jin, M. Choi, L. Wang and S. Choi, "Fast scanning schemes for IEEE 802.11 WLANs in virtual AP environments," Computer Networks, vol. 55, pp. 2520– 2533, July 2011.
8. Y. Grunenberger and F. Rousseau, "Virtual access points for transparent mobility in wireless LANs," in Proc. IEEE Wireless Communications and Networking Conference, April 2010, pp. 1-6.
9. S. Jin, M. Choi, and S. Choi, "Multiple WNIC-based handoff in IEEE 802.11 WLANs," IEEE Communication Letters, vol. 13, no. 10, pp. 751-754, Oct. 2009.
10. Yi-Cheng Chan and Dai-Jiong Lin, "The Design of an AP-Based Handoff Scheme for IEEE 802.11 WLANs,"J.e-Education, e-Business, e-Management and e- Learning, vol. 4, no. 1, Feb. 2014

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 5 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Qos Provisioning for Energy Efficiency in Mobile Ad-Hoc Network

By Sridhara S B & Dr. Ramesh B
RGIT/VTU University, India

Abstract- In mobile ad-hoc networks Quality of Service (QoS) of a multicast routing protocol is one of the most key performance metrics. Slotconditions and network topology frequently change (Topology dynamic), and in order to achieve a certain level of QoS, complexalgorithms and protocols are needed. Network graph conditionsare neglected during the design of aexisting multicast protocol. However, vulnerability against network graph errors can severely affect theperformance of a multicast protocol. To address this here the author proposesanenergy efficient network graph pre-processing approach to enable traffic engineering and enhance the performance of energy efficiency in terms of network efficiency by QoSprovisioning, to cater the multicast routing issue in MANETS.In this approach prioritized admission control (PAC) scheme is implemented to improvise D2D (Device to Device) communications into cellular network to overcome the limitations of MANETs.

Keywords: ADHOC, wireless cellular/mesh network, D2D, routing, multicasting.

GJCST-E Classification : C.1.3 C.2.6

Strictly as per the compliance and regulations of:

Qos Provisioning for Energy Efficiency in Mobile Ad-Hoc Network

Sridhara S B[α] & Dr. Ramesh B[σ]

Abstract- In mobile ad-hoc networks Quality of Service (QoS) of a multicast routing protocol is one of the most key performance metrics. Slotconditions and network topology frequently change (Topology dynamic), and in order to achieve a certain level of QoS, complexalgorithms and protocols are needed. Network graph conditionsare neglected during the design of aexisting multicast protocol. However, vulnerability against network graph errors can severely affect theperformance of a multicast protocol. To address this here the author proposesanenergy efficient network graph pre-processing approach to enable traffic engineering and enhance the performance of energy efficiency in terms of network efficiency by QoSprovisioning, to cater the multicast routing issue in MANETS.In this approach prioritized admission control (PAC) scheme is implemented to improvise D2D (Device to Device) communications into cellular network to overcome the limitations of MANETs. It enables to enhance the estimated network performance which is gained from offloading cellular traffic onto D2D architecture. Extensive simulation has been carried out for various parameters such as throughput, slot utilization and energy efficiencyand the results show that the proposed approach can significantly improve the performance of QoS multicast routing in MANETs in order to enhance device battery life and overall network energy efficiency. The architecture shows that D2D communications is forming an ad-hoc structure in cellular network to provide a significant improvement in QoS efficiency andalso enable overall network capacity performanceby individualuser's energy optimization.

Keyword: ADHOC, wireless cellular/mesh network, D2D, routing, multicasting.

I. Introduction

As Telecom administrators are finding difficulties to fulfil the current requests of portable clients, new information intensified applications are created for standard use of versatile client, for example, proximity-aware administration services, however,4G phone advancements, which have exceptionally productive physical and MAC (Medium Access Control) layer execution are as yet falling behind portable clients expanding information requests. Thus scientists are searching for new strategies to change the customary specialized technique for cell system. Gadget (User) to Device (D2D) framework is one of such technique that give off an impression of being an empowering segment in future era cell network.D2D correspondence in cellular systems is defined as immediate correspondence between two portable clients without crossing the Base Station (BS) or centre system. D2D correspondence is by and large non-straightforward to the cell system and it can happen on cell range i.e., in band or unlicensed range i.e., out band. In a customary cell arrange, all interchanges ought to be done by means of base station (BS) regardless of the possibility that both imparting gatherings are in reach for D2D correspondence. These structural planning suits the ordinary low information rate versatile administrations, for example, voice call and instant message in which clients are not frequently sufficiently close to have direct correspondence. Let us assume, portable clients in today's phone systems utilize high information rate administrations, for example, feature sharing, gaming, and vicinity mindful person to person communication in which they could be in reach for direct interchanges Hence, D2D correspondences in such situations can profoundly expand the otherworldly efficiency of the system. By and large the benefit of D2D correspondences is not just constrained to upgraded ghostly efficiency. D2D correspondences can possibly enhance throughput, energyefficiencyand effective scheduling. Figure 1 shows structural engineering of imagined D2D correspondence.

Author α : Sridhara S.B., Assistant Professor, Dept of Electronics and communication Engineering, Rajiv Gandhi Institute of technology, Bangalore, India. e-mail: sridharasb1947@gmail.com
Author σ : Dr.Ramesh B., Professor. Dept of Computer science and engineering, Malnad college of Engineering, Hassan, India.
e-mail: sanchara@gmail.com

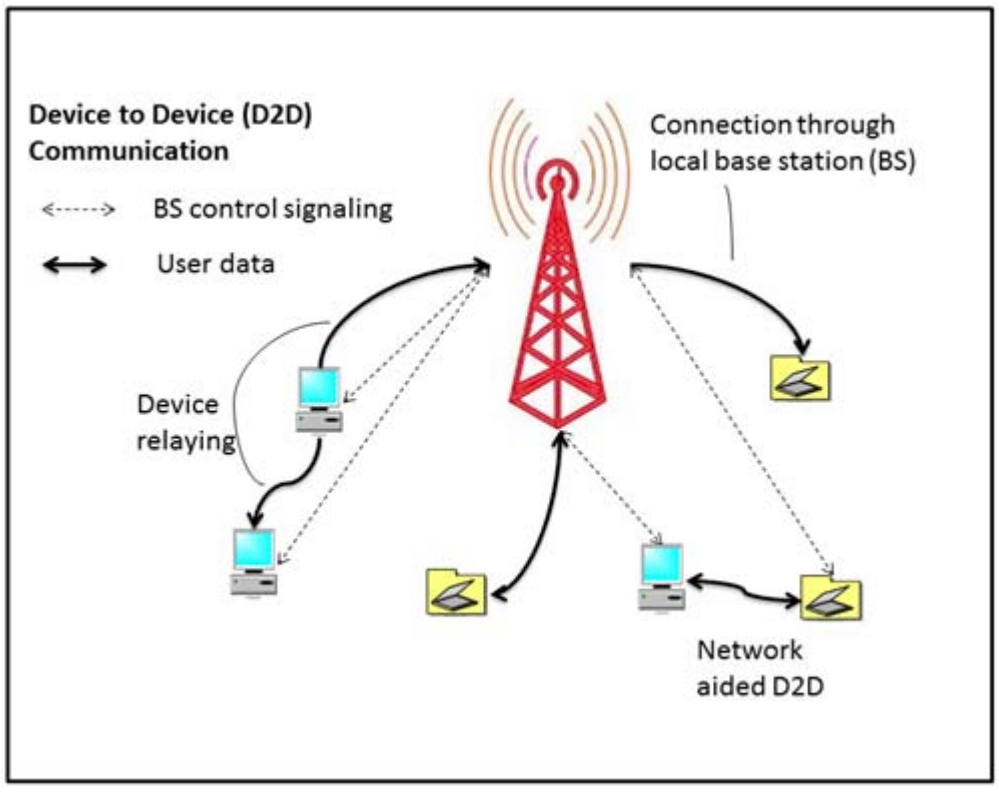


Figure 1 : Architecture of envisioned D2D ommunication

D2D correspondence was first proposed in Y.D et al., [16] to empower multihop transfers in cell systems. In T. Han et al., [2], B. Kaufman et al., [3], K. Doppler et al., [5], K. Doppler et al.,[6] scholars inspected the probability of D2D correspondences for enhancing ghastly efficiency of cell systems. In J. Du et al., [7], B. Zhou et al.,[8] other conceivable D2D utilization cases were presented in the writing, for example, multicasting and shared correspondence in L. Lei et al., [9], feature scattering in K. Doppler et al., [3] N. Golrezaei et al., [10], N. Golrezaei et al.,[11], J. C. Li et al., [12], machine-to-machine (M2M) correspondence in N. K. et al., [13] and cell of floading X. Bao et al[14]. The first endeavour to executing D2D correspondence in a cell system was made by Qualcomm's FlashLinQ X. Wu et al., [15] which is a PHY/MAC system construction modelling for D2D interchanges underlaying cell systems. FlashLinQ exploits OFDM/OFDMA advancements and circulated planning to make an efficient technique for timing synchronization, peer disclosure, and connection administration in D2D-empowered cell systems. Furthermore 3GPP (3rd Generation Partnership Project) is additionally examining D2D correspondences as Proximity Services. With fast development of radio access procedures and cell phones, a mixed bag of transmission capacity hungry applications and administrations are slowly moved to versatile systems, prompting an exponential increment in information activity in portable systems. The versatile information activity endures two noteworthy issues to current portable systems, as the critical information increment clogs versatile systems and prompts a long postpone in substance conveyance.T. Han et al., [1] and a nonstop stream of versatile movement bring about high increment in vitality utilization in versatile systems for giving higher system limit.T. Han et al., [17]. Portable activity offloading, which is referred to as using shared system correspondence methods to convey versatile movement, is a promising procedure to enhance blockage and lower the vitality utilization of portable systems.T. Han et al., [1]. Taking into account the system access mode, the portable activity offloading plans can be separated into two classes. The primary class is the foundation based versatile activity offloading and the second classification is the specially appointed based portable movement offloading, which refers to applying gadget to-gadget (D2D) interchanges as an underlay to offload portable activity from BSs. By presenting Internet of Things (IoT) innovations, brilliant gadgets inside of vicinity have the capacity to associate with one another and structure a correspondence system. Information movement among the gadgets can be offloaded to the interchanges arranges as opposed to conveying through BSs, by empowering D2D correspondences, some client gadgets/User Devices (UDs) download substance from BSs while alternate UDs may recover the substance through D2D associations with their companions. Along these lines, D2D correspondences simplicity movement blockage and reduce the vitality utilization of versatile systems. In

this paper, the author propose a novel network graph processing way to deal with empower movement designing and improve the execution of energy proficiency regarding system life time by QoS provisioning, to addressfare multicast routing issue in MANETS. This methodology fused the organized affirmation control plan to communicate D2D interchanges into cell system to conquer the restrictions of MANETs. In this affirmation control is an essential capacity for the procurement of QoS as it figures out which parcel is permitted to enter and which bundle is not permitted to go into the system. The choice may be in view of numerous variables, for example, what may be the result of permitting a bundle to go into the system. The approach is improving the evaluated system execution which is picked up from offloading cell movement onto D2D structural engineering.

a) Issues and challenges

In an adhoc system the cell phones (devices) are associated through remote connections that are more inclined to lapses when contrasted with their wired connections. There are issues, for example, hidden terminal, multipath distorting, and so forth. Rather than a wired system, there are no different switches, consequently, the cell phones need to course parcels of each other towards their last destination. Generally cell phones are furnished with omni-directional reception gadgets/devices, and afterward, transmissions of a hub are heard by hubs in its encompassing. This causes an issue, for example, hubs need to facilitate among themselves for transmissions through a mutual channel. At the end of the day, a hub can't settle on its own about the season of the start of a transmission in light of the fact that the channel may be involved by another hub in its encompassing. Thus the time taken in sitting tight for the transmission relies on who are the other neighbouring hubs going after the channel or there may be numerous bounces from an offered source to a destination in an ad-hoc system and at every jump hubs may go after the channel. Because of channel dispute, it is hard to give any guarantees about the end-to-end delays. Be that as it may, there is no such issue in wired systems as the channel is not shared ,On the other hand, the topology of an ad-hoc system changes rapidly because of either development of cell phones or depletion of battery force. It may influence QoS assurances gave by the system in light of the fact that an adjustment in the topology of the system may require to rediscover the courses adding to the latencies and hence influencing the QoS. It might likewise happen that the newfound courses are longer than the courses accessible before the topological change which will influence the QoS all the more seriously, as the assets that were saved for a stream before the topological change are no more held, they must be saved along more up to date courses. It might likewise happen that the measure of assets needed by the information stream or application is no more accessible, including further latencies and influencing the QoS. In this manner, another issue included in the procurement of QoS in versatile ad-hoc systems is the way to handle changes in the topology of the system. Extra issue if there should arise an occurrence of portable specially appointed systems is that the assets of participating hubs are constrained. Along these lines, a convention that requires broad calculations and correspondences may not be a decent alternative in such systems. Hence, a convention for giving QoS in specially appointed systems ought to be light-weight beyond what many would consider possible and ought to have the capacity to use assets in a productive and viable way.

II. Related Work

A large portion of the ordinary multicast conventions are intended for expanding the throughput or minimizing the end-to-end delay. At the point when QoS is viewed as a few conventions may be inadmissible because, the absence of the asset and the exorbitant calculation overhead Luo Junhai et al., [18]. A few calculations Luo Junhai et al., [19] give heuristic answers for the NP-(Nondeterministic Polynomial) complete compelled Steiner tree issue, which is to discover the deferral obliged minimum expense multicast trees. These calculations however are not down to earth in the internet environment in light of the fact that they have unreasonable processing overhead, oblige information about the worldwide system state, and don't handle element groupenrolment. InLi Layaun et al., [20] gives different guarantees to fulfilling various imperatives however it doesn't keep up any worldwide system state. In J. H. Cui et al., [21] another versatile QoS multicast directing convention that has little correspondence overhead and obliges no state outside the multicast tree is proposed. Huayi Wu et al., [22] propose a QoS Multicast Routing convention (QMR) with an adaptable cross breed plan for QoS multicast routing ,QMR is a lattice construct convention which is set up in light of interest to unite bunch individuals and gives QoS ways to multicast bunches. The QMR convention coordinates data transfer capacity reservation capacity into a multicast steering convention with the suspicion that accessible transmission capacity is consistent and equivalent to the crude channel transmission capacity. Affirmation control system is utilized to keep middle of the road hub from being over-burden and reject solicitations of new sources if there is no accessible transmission capacity. In S.S. Manvi et al., [23] An operator based multicast directing plan (ABMDP) in MANETs, which utilizes an arrangement of static and portable specialists for course disclosure and upkeep is proposed but it doesn't consider the various QoS imperatives. Ad-hoc construct portable (packet

traffic) activity offloading depend with respect to D2D interchanges to telecast information parcels. Rather than downloading information specifically from BSs, UDs may recover substance from their neighbouring UDs. In B. Han et al., [24] proposed a system to choose a subset of User Equipment's (UEs) in light of either UEs' exercises or motilities, and to convey substance to them through cell systems, and let these UEs further disperse the substance through D2D correspondences to alternate clients. In A. Mashhadi et al., [25] the creator proposed a proactive storing system for UEs keeping in mind the end goal to offload the versatile activity. At the point when the nearby stockpiling does not have the asked for substance, the proactive reserving system will set an objective deferral for this solicitation, and investigates chances to recover information from the neighbouring UEs. The proactive store system demands information from cell systems when the objective deferral is damaged. To support versatile clients take an interest in the activity offloading, in X. Zhuo et al., [26] proposed a motivator system that incentive clients to influence their deferral resistance for cell information offloading.

III. Proposed System

a) Wireless cellular network (WCN)

In remote cell system (WCN) Base station (source) shape a base of spine for destination hubs, for the most part source have negligible portability and work like a system for settled switches and get joined by remote connections, for example, IEEE 802.11.even some source hub have passage usefulness since they are associated with web with physical wire. In any case, each source hub is furnished with movement accumulation gadget, for example, 802.11 entrance point that communicates with every destination hubs. The source hub conveys totalled information movement of destination hubs to and from the web. In this paper, spine i.e. source hub is framed by 802.11.Usually a switch is outfitted with different remote interfaces, each of which is comparing to one remote channel. These remote channels have diverse components, in light of the fact that remote interfaces are running on distinctive frequencies and based on either the same or distinctive remote access innovations, for example, IEEE 802.11a/b/g/n. Continuously situation, to combine two switches with higher data transfer capacity limit, different remote channels can be set up between two switches. Expecting that in cell arrange the remote connection between two switches has altered data transfer capacity limit for the reasons, for example, backing of base i.e., a spine can be manufactured amongst remote switches I. F. Akyildiz et al., [27]and procedures, for example, directional receiving wire and pillar framing can be utilized to enhance the execution of remote correspondence and keep up the "remote connections" , On the other hand, if the omni-directional reception apparatus is utilized, "remote connections" can in any case be built however topology control N. Li et al., [28],for the limit of remote connection, a "successful limit" methodology has been created to unravel the outline of energy efficient QoS backing in remote system. In such a case, the powerful limit of the remote connection, which is settled, can be utilized for QoS steering, despite the fact that the genuine limit of the remote connection can in any case be changing lastly, because of the multifaceted nature of the physical layer and medium access control (MAC) layer, numerous current studies in the literature additionally expect that the connection limit is altered.

b) Energy Efficient QoS Multicast Routing

Multicast is an effective approach to transmit information from one source hub to a gathering/group of destination hubs. In later year's quick development of group oriented applications in remote/wireless environment, it gets to be vital to bolster multicast in wireless cell network systems. Since multicast client normally require energy efficient QoS ensured services, which thus depends on QoS multicast routing. Once the cellular remote/wirelessnetwork is conveyed the spine can be representedby ainfrastructure/ networkgraph$NG(V,E)$. In the graph, hubs (V) stand for correspondence endpoints, edges (E) stand for correspondence links. To perform QoS directing, allot every edge a weight, indicated by $W_{lQoS} = (w_{lc}, w_{lb}, w_{ld})$ where w_{lc} denotecost, w_{lb} data transfer capacity limit andw_{ld}transmission deferral/delay of connection/link$l$ separately. In this proposed model to encourage the routing process, the different remote/wirelesschannels between two switches are taken care by consolidating after two methodologies. In the first place, if these wireless channels utilize the same convention and have indistinguishable information transmission execution, then the channels are essentially converged into one virtual connection. In any case, the traffic burden routed on the virtual connection would be equitably circulated on distinctive channels at the MAC layer. Then again, if numerous remote/wireless channels utilize diverse conventions or have unmistakable information transmission execution because of the assorted qualities of channel conditions on distinctive working frequencies, then every wireless channel will considered as a virtual connection and an auxiliary/assistant hub is added to it. From the point of view of routing conventions, auxiliary hubs are not quite the same as switches in light of the fact that they don't create any traffic load and can't assume the part of source or destination. A multicast association solicitation can be portrayed as$M_{req} = (s, D, QoS)$where s is the source hub, $D = \{d_1, d_2 \dots \dots \dots d_n\}$is a set of destination hubs,

and QoS is a set of QoS necessities, for example, data transfer capacity and deferral/delay bound. At the point when deploying MANET for Internet access, the multicast source hub is typically one of the portal switches/gateway, for example, $NG1, NG2$ and $NG3$. The multicast tree T for solicitationM_{req} is a subtree of $NG(V, E)$ which roots from s, contains every one of the hubs of D, and can meet the energy efficient QoS imperative QOS. In this manner, the expense (cost) of multicast tree T is given by following equation.

$$C_T = \sum_{l \exists T} w_{lc} \quad (1)$$

To set up a multicast association, for the most part QoS multicast routing algorithm will be utilized to locate the ideal multicast tree that has the least cost while fulfilling all QoS prerequisites. This said QoS multicast routing issue is otherwise called compelled Steiner tree issue, which has been ended up being NP-complete. In [29] heuristic calculations have been created to take care of obliged Steiner tree issue. These heuristic calculations can be characterized into two classes the centralized algorithm and the distributed algorithm. As most algorithm proposed so far have a place with centralized class, proposed strategy additionally address the centralized QoS multicast directing algorithm. Some late studies proposed to bolster multicast correspondence utilizing network coding [30], where all connections in the system may be used, rather than a tree. Despite the fact that network coding can accomplish the best throughput hypothetically, it requires the change of existing packet sending components, which is not a simple task. Here the routing policy of obliged Steiner tree and its heuristic algorithm is considered for QoS multicast routing, the input/information is the link/connection state graph. The principle distinction between link state graph and network foundation/infrastructure graph is that, in connection/link state graphw_{lb} signifies the leftover data transfer capacity on connection/link which can change every now and then, while in network framework/infrastructuregraph w_{lb} denotes the transmission capacity limit of the connection/link/ which is a steady/constant.

c) Energy Efficient Network Graph Pre-processing

Existing QoS multicast transmission (routing) are intended to discover ideal trees for multicast associations and they don't guarantee that the system runs productively/efficiently. To better use system assets in remote cell system environment (WCN), traffic engineering (TE) can be used to enhance asset effectiveness by accomplishing burden adjusting over the network system. Then again, past traffic engineering (TE)mechanism may not be specifically used to connect Wireless cell system (WCN). In this approach two central point in wireless cell system (WCN) are considered in traffic engineering deployment: 1) the transmission capacity prerequisites of uses are various and a few applications require extensively higher transfer speed than that of the others; and 2) the limits of numerous remote connections are not altogether huge, contrasted with the transfer speed necessity of high-information rate applications. As another issue that ought to be taken care of is normal burden adjusting plan which could prompt data transfer capacity discontinuity, thus hurts the acknowledgment of high transmission capacity associations and results in access injustice. At the point when transfer speed fracture happens, low-transmission capacity associations can at present perhaps get to the system, while most high data transfer capacity associations are blocked. To manage the aforementioned difficulties in wireless cell system (WCN), here the authors propose a network graph pre-processing methodology taking into account PAC policy. The fundamental thought of the proposed methodology is the point at which another (user request) association solicitation arrives, the first network graph is pre-generated and after that another new graph is produced. In this work, the authors utilize organized affirmation control (i.e. PAC) to accomplish traffic engineering (TE). Next, the new network graph is used as the info of a QoS multicast transmission algorithm to discover the QoS ensured tree. In this work authors include network graph pre-preparing as a methodology just before the QoS multicast transmission algorithm. In the literature survey, most existing QoS transmission/routing algorithm regard transmission capacity necessity as a non-added substance requirement, which can be effortlessly managed by editing from the network graph every one of the connections whose remaining transfer speed is not exactly the imperative. To coordinate traffic engineering (TE) component into QoS multicast routing/transmission, we adjust the method for data transmission requirement taking care of, and outline another organized affirmation control model (PAC). In this model, distinctive confirmation control approaches can be utilized on diverse connections/links and group association demands into two categories:1) high data transfer capacity connection/associations, and 2) low-transmission capacity associations. To do network graph pre-processing, a few connections/links are selectedfrom the NG pre-processing as best/special connections/link, and rest of the connections/link are characterized as conventional/normal connections/links. Here, best/special connections/link is intended to predominantly acknowledge high-transfer speed associations. Naturally, the great possibility for extraordinary connections is the ones that have high data transmission limit and are midway/centrally situated in the system. Indeed, even low-data transfer capacity

associations can likewise get to the exceptional/best connections, while high-transmission capacity associations are given more need on them. The data transfer capacity designation relies upon the need of the association, as well as the traffic burden profile in the network system. Case in point, high-data transfer capacity associations could be assigned a little measure of transmission capacity on exceptional/best connections if their traffic burden is light. Then again, low-data transmission associations could be dispensed a lot of transfer speed on special connections if their traffic burden is expansive. Organized affirmation control approach (PAC) is utilized to offer inclination to high-transmission capacity associations. At the point when another association (connection) solicitation (request) comes, the organized confirmation control approach (PAC) is utilized to make transfer speed affirmation test just on extraordinary/best connections. Thus for disparity, no action is made on common (normal) connections, if the organized confirmation control (PAC) arrangement chooses to dismiss the association ask for on some best connections, these connections are then expelled from the network graph. At that point pruned network graph is characterized as pre-generated/pre-process network graph, in which some extraordinary/best connections may vanish while every single customary/normal connection isretained. When the network graph pre-generation/processing is finished, the transmission/routing algorithm uses the pre-generated/processed as the data to discover a QoS ensured multicast tree for the association/connection demand/request. Utilizing network graph pre-processing, high-transfer speed associations and low-transmission capacity associations may have diverse pre-processed graph. Notwithstanding for two association asks for that have the same source and destinations, there is a probability to have distinctive QoS ensured multicast trees, if their data transmission prerequisites are not the same. Subsequently, high-transfer speed activity can be basically accumulated on unique/special connections, while low-transmission capacity movement can be dispersed on conventional\ordinary connections. Because of this element, theproposed network graph pre-processing methodology as shown in figure 2 can furnish energy efficient QoS multicast routing with a better load adjusting ability and can keep away from data transfer capacity fragments.

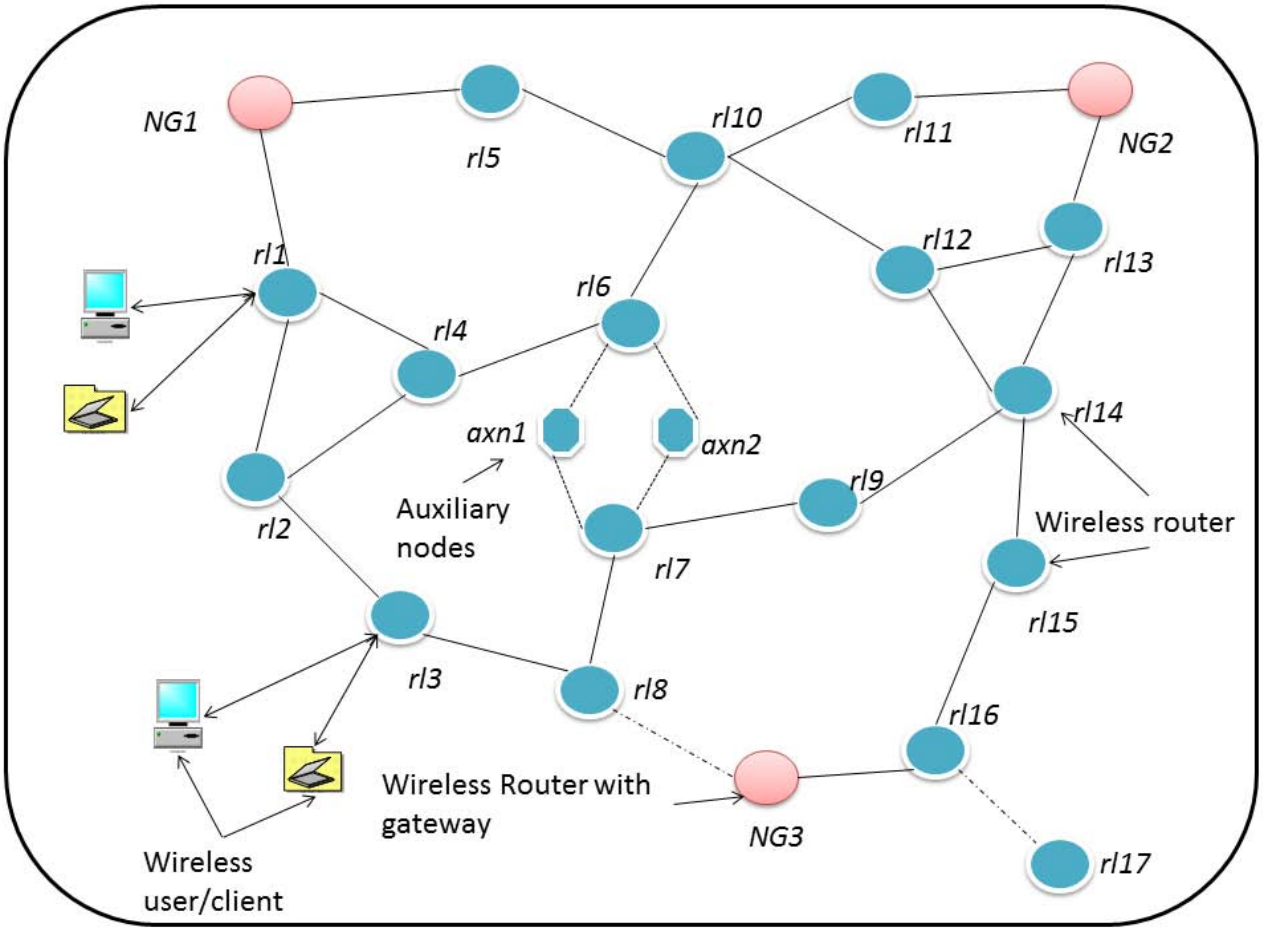


Figure 2 : Proposed Energy Efficient QOS Provisioning Model

d) Special Link Selection

In this proposed methodology special link (connection)selection and organized affirmation control (PAC) are two vital steps to accomplish good and efficient performance. Initiallywe investigate the speciallink (connection)selection issue by considering two noteworthy criteria in picking extraordinary (best) connections. Firstly, extraordinary (special) connections ought to be halfway (centrally) situated in the wireless network topology and furthermore, special link (connections) must have high data transfer capacity limit. With these two criteria, a Shortest Path (SP)based model to pick special connections from wireless network framework/infrastructuregraph is produced, as shown in Algorithm 1.

Algorithm 1 Shortest Path Based Special Link Selection

Step 1 : Start

Step 2 : Input the bandwidth threshold $(Bw_{\mathcal{T}})$ and number of special links $(N_{\mathbb{Spl}})$

Step 3 : for any router pair (rl_1, rl_2) in network infrastructure graph do

Step 4 : use w_{lc}as metric to find special link i.e. $Spl(rl_1, rl_2)$ which represents the shortest path between rl_1 and rl_2

Step 5: for any link $l \in Spl(rl_1, rl_2)$do

Step 6 : $fl = fl + 1;$ where fl is the frequency that link l emerges in the shortest paths

Step 7: end for

Step 8: end for

Step 9: In network infrastructure graph, select the links whose bandwidth capacity is higher than $Bw_{\mathcal{T}}$ to form set $L_{\mathcal{T}}$;

Step 10 : From $L_{\mathcal{T}}$, choose the top N_{Spl} links with the highest value of fl as special link;

Step 11 : End

To meet the first standard/criteria, just the connections emerging/rising most often in the shortest path, will be picked as special connections and for second measure a data transfer capacity limit edge$Bw_{\mathcal{T}}$ is used in this algorithm. Any connection with a transfer speed limit lower than $Bw_{\mathcal{T}}$ will be disposed of furthermore the quantity of exceptional/special connections meant byN_{Spl}can be balanced by network director/administrator as indicated by the extent of high data transmission activity in the system. While the info parameters $Bw_{\mathcal{T}}$and $N_{Spl}$are intended for the multicast environment. In remote cell (WCN), the source hub of a multicast session more often than not is one of the Internet passages/ gateway, for example $\{NG1, NG2, NG3 \ldots \ldots NGn\}$. On the off chance that theproposed objective is to choose special connections for unicast directing,it is just need to consider the shortest path from the Internet passages/gateway. In any case, in network set-up graph all the shortest path are considered, following for multicast transmission, any switch is conceivable to serve as intermediate hub in multicast tree as shown in figure 2 and figure 3.

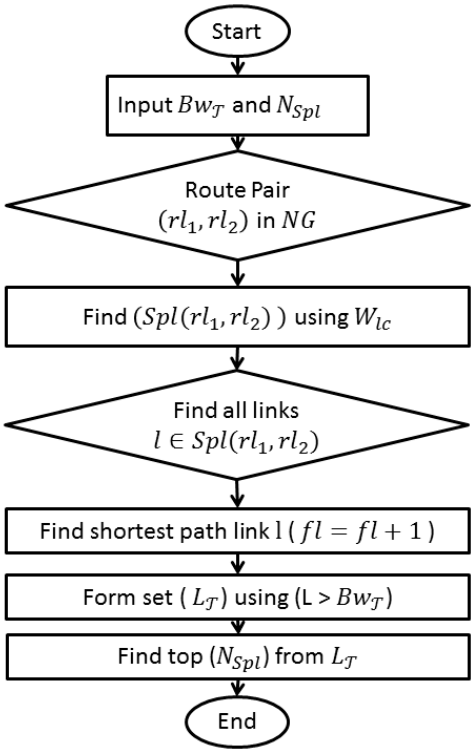


Figure 3 : Flow diagram of proposed shortest path based special link selection

IV. Simultion Result and Analysis

The system environment used is windows 7 enterprises 64-bit operating system. Authors have used dot net general purpose simulator which is based on C# programming and used dot net framework 4.0 visual studios 2010 and conducted simulation study on following parameter for slot/link selection, throughput and energy efficiency and compared the proposed energy efficient QoS PAC model with existing D2D (Device to Device) protocol.

a) Slot success ratio analysis

From figure 4 the number of users varied from 6, 12, 18, 24 and 30 and the simulation result show that the proposed PAC model improved by 13.8%, 11.8%, 10.6%, 10.1% and 12% respectively over existing D2D model.

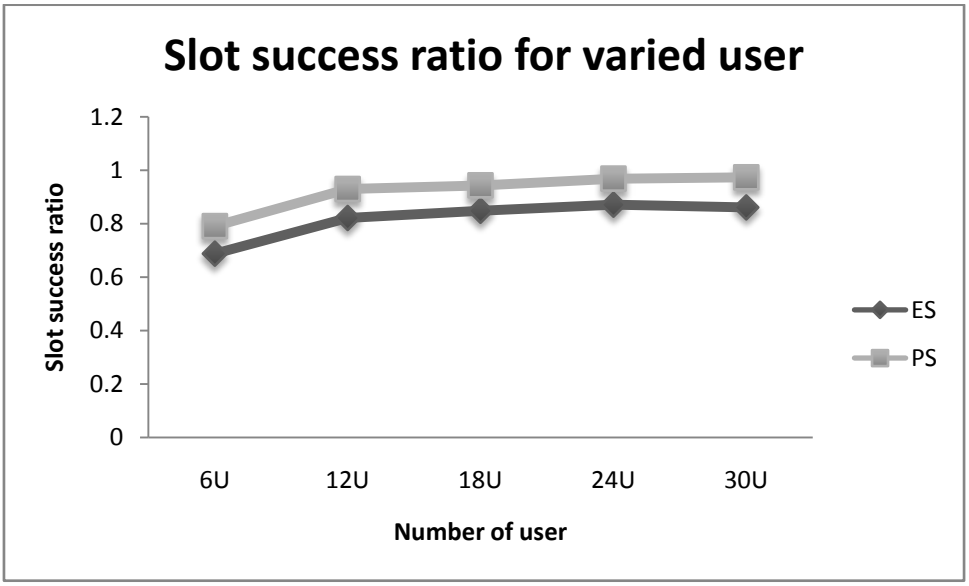


Figure 4 : Slot success ratio for varied user

From figure 5 itshows that the proposed PAC model performs better than existing D2D model in term of slot success ratio. The experimental result shows that proposed model slot/link utilization ratio is improved by 12 % over the existing model

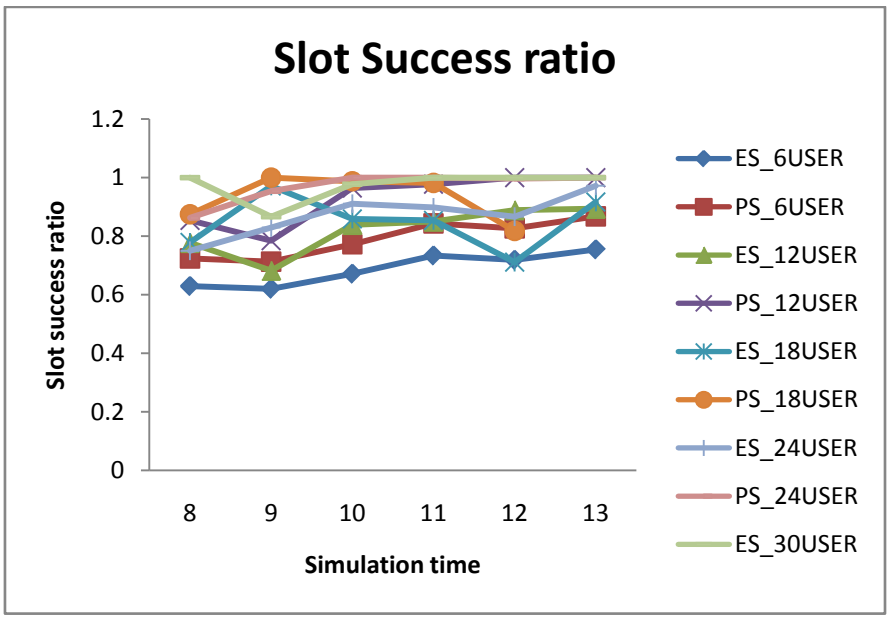


Figure 5 : Slot success ratio

b) Throughput analysis

In figure 6 the throughput efficiency is analysed by varying the number of user from 6, 12, 18, 24 and 30 and the simulation result show that the proposed PAC model improves the throughput efficiency by 7.8%, 8.2%, 8.34%, 8.38% and 7.88% respectively over existing D2D mode

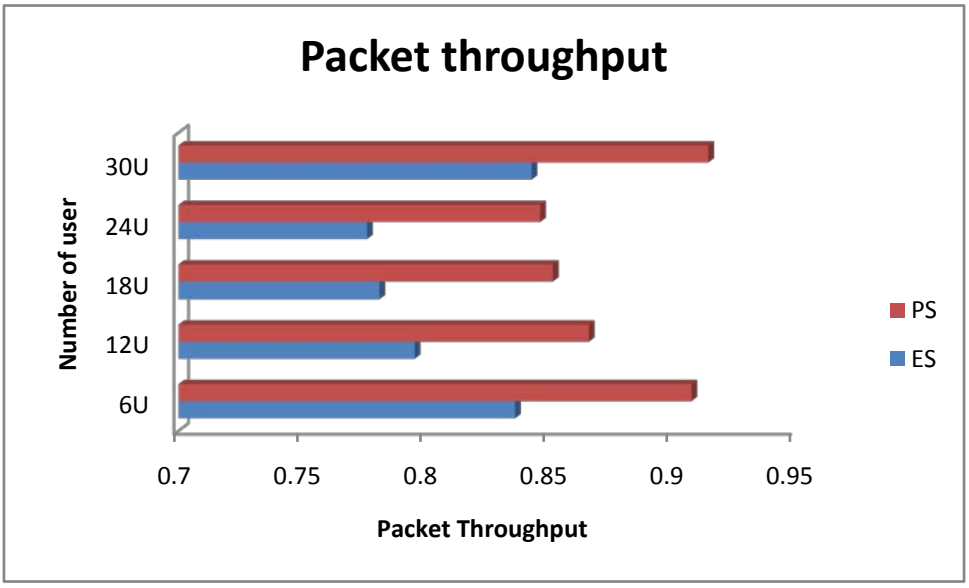


Figure 6 : Packet throughput

Figure 7 shows that the proposed PAC model performs better than existing D2D model in term network throughput efficiency. The experimental result shows that proposed model throughput efficiency is improved by 8.58 % over the existing model.

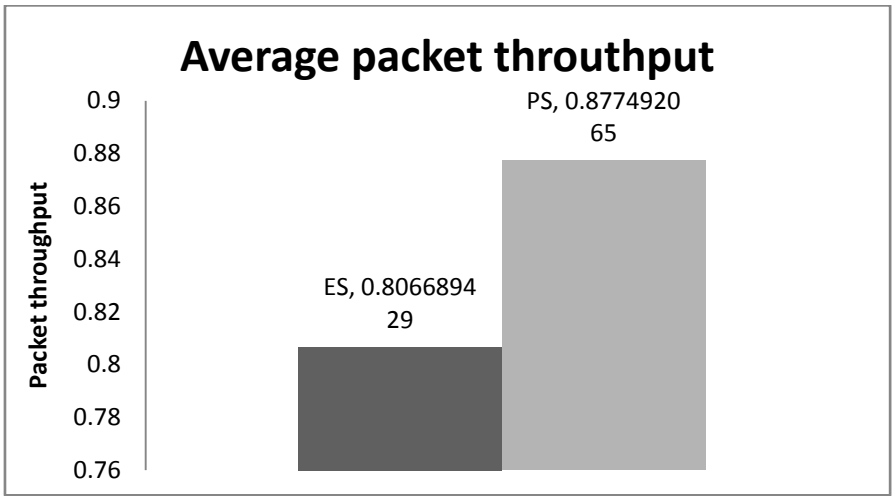


Figure 7 : Average packet throughput

c) Energy efficiency analysis

From figure 8 it shows the network energy efficiency by varying the number of user from 6, 12, 18, 24 and 30 and the simulation result show that the proposed PAC model improves the network energy efficiency by 23.62%, 24.35%, 26.32%, 23.21% and 34.56% respectively over existing D2D model.

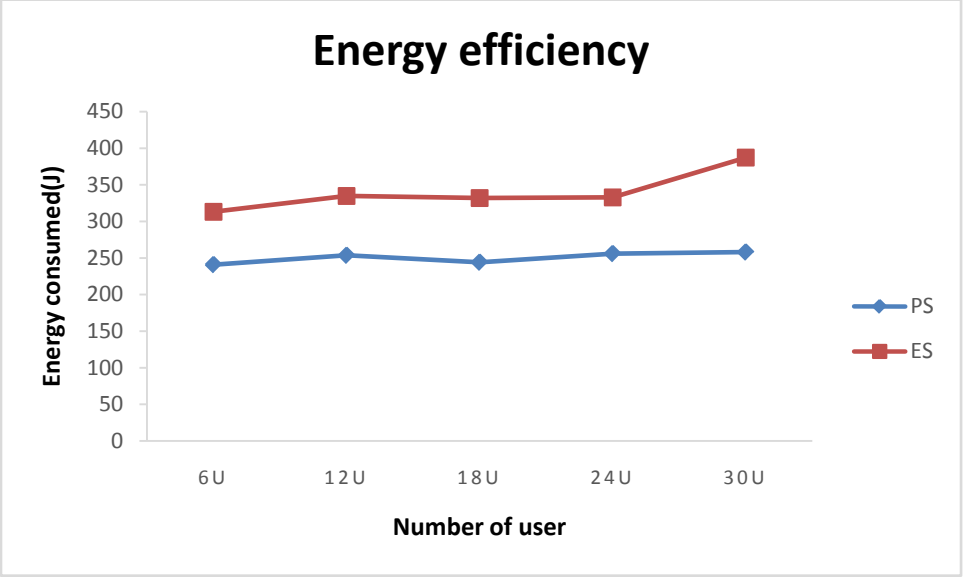


Figure 8 : Energy efficiency

The figure 9 shows that the proposed PAC model performs better than existing D2D model in term network energy efficiency. The experimental result shows that proposed model energy efficiency is improved by 27 % over the existing model.

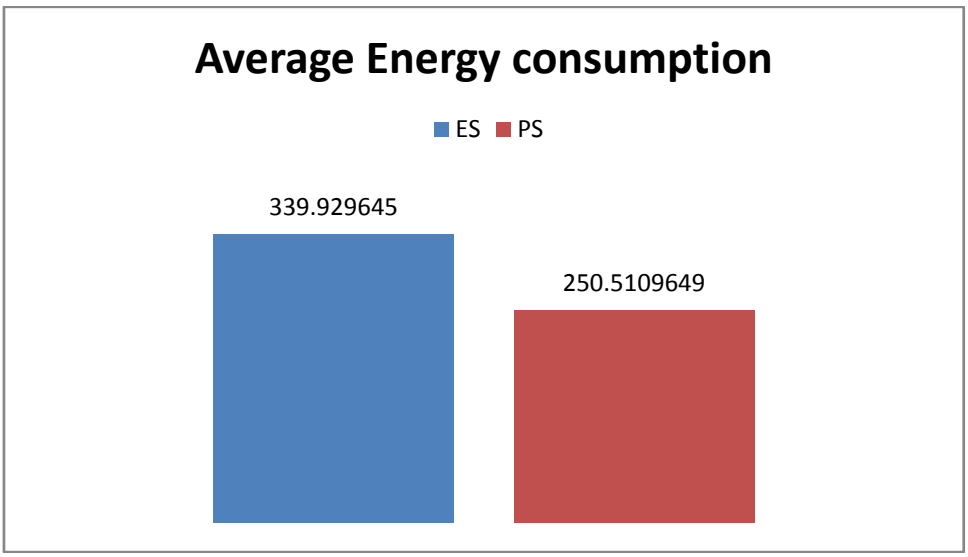


Figure 9 : Average energy consumption

In figure 10 we have obtained the average energy consumed by proposed model by varying simulation time from 200 to 1000 seconds for varied number of user and found that the average minimum energy was around 180 joules and the maximum average energy was around 322 joules.

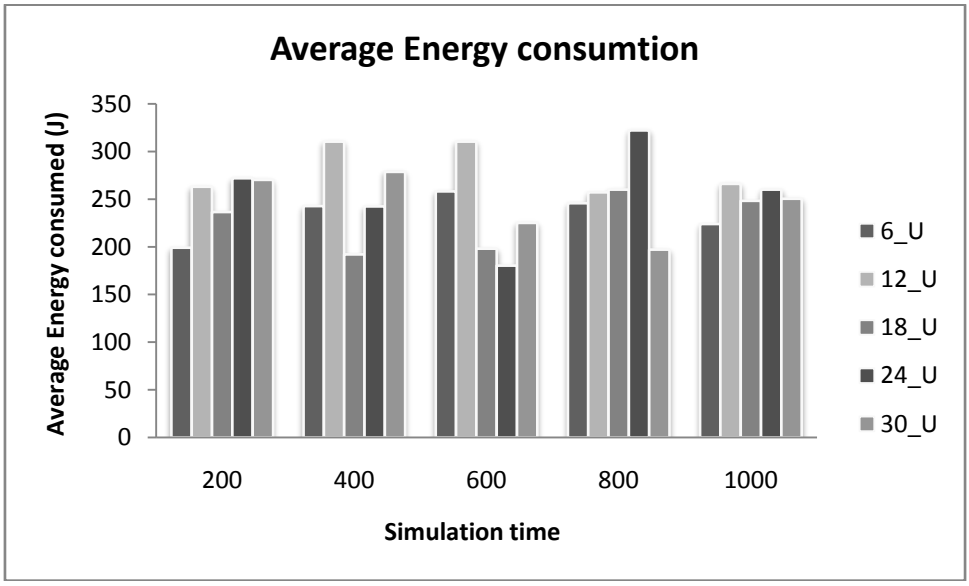


Figure 10 : Average energy consumption v/s simulation time

V. Conclusion

In this paper, a Traffic Engineering (TE) enhanced model is proposed and implemented to improve the performance efficiency of QoS multicast routing algorithms in mobile ad-hocenvironment. Particularly, the author has proposed a new approach of network graph pre-processing based on PAC (Prioritized Admission Control) to achieve a desirable traffic engineering capability from the admission control scheme, precisely, a set/group of links isselected from the ad-hoc network as special links, where PAC policy is then conducted. A special link/Best link will be removed from the network graph if the connection request does not pass the PAC test. As a result, different connections (user network) may have different pre-processed ad-hoc network graphs, and the traffic/packet load can be evenly distributed in the ad-hoc network. Simulation results demonstrate that the new approach can obtain good performance in terms of link/slotutilization, energy efficiency, and network throughput. Further the work can be extended to develop an optimal priority gain policy considering varied network traffic load and different network services (UGS, RTPS, NRTPS (such as VoIP, MPEG video etc..)) and then design a traffic load estimating mechanism/model to accurately track the traffic summary/profile in mobile ad-hoc network, so that PACpolicy can be adaptive to the varying traffic scenario/patterns.

References Références Referencias

1. T. Han, N. Ansari, M. Wu, and H. Yu, "On accelerating content delivery in mobile networks," *IEEE Communication surveys & Tutorials, vol. 15, no. 3, pp. 1314–1333, 2013*.
2. Kaufman B.; Aazhang B., "Cellular networks with an overlaid device to device network," *Signals, Systems and Computers, vol.1537, no.1541, pp.26-29, 2008.*
3. K. Doppler, M. Rinne, C. Wijting, C. Ribeiro, and K. Hugl "Device-to- device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine, vol. 47, no. 12, pp. 42–49, 2009.*
4. Doppler K.; Rinne M.P.; Janis P.; Ribeiro C.; Hugl K., "Device-to-Device Communications; Functional Prospects for LTE-Advanced Networks," *Communications Workshops,IEEE International Conference on , vol., no., pp.1,6, 14-18 June 2009.*
5. A. Osseiran, K. Doppler, C. Ribeiro, M. Xiao, M. Skoglund, and J. Manssour, *"Advances in device-to-device communications and network coding for IMT-Advanced," ICT Mobile Summit, 2009.*
6. T. Peng, Q. Lu, H. Wang, S. Xu, and W. Wang, "Interference avoidance mechanisms in the hybrid cellular and device-to-device systems," *IEEE PIMRC,vol. 19, no. 3, pp. 617–621,2009.*
7. J. Du, W. Zhu, J. Xu, Z. Li, and H. Wang, "A compressed HARQ feedback for device-to-device multicast communications," *IEEE VTC-Fall,vol. 15, no. 3, pp. 1–5, 2012*.
8. B. Zhou, H. Hu, S.Q. Huang, and H.H. Chen, "Intracluster device-to- device relay algorithm with optimal resource utilization," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2315–2326, 2013.
9. L. Lei, Z. Zhong, C. Lin, and X. Shen "Operator controlled device-to- device communications in LTE-advanced networks," *IEEE Wireless Communications*, vol. 19, no. 3, pp. 96–104, 2012.
10. N. Golrezaei, A. F. Molisch, and A. G. Dimakis, "Base-station assisted device-to-device

communications for high-throughput wireless video networks," *IEEE* Communication Magazine,vol. 10, no. 3 pp. 7077–7081, 2012.
11. N. Golrezaei, A. G. Dimakis, and A. F. Molisch, "Device-to-device collaboration through distributed storage," *IEEE* Communication Magazine, vol.51, no.4, pp.142-149, April 2013.
12. J. C. Li, M. Lei, and F. Gao, "Device-to-device (D2D) communication in MU-MIMO cellular networks," *Global Communications Conference (GLOBECOM), vol. 3583, no. 3587, pp.3-7*, 2012.
13. N. K. Pratas and P. Popovski, "Low-rate machine-type communication via wireless device-to-device (D2D) links," *arXiv preprint arXiv: 1305.6783*, 2013.
14. X. Bao, U. Lee, I. Rimac, and R. R. Choudhury, "DataSpotting: offloading cellular traffic via managed device-to-device data transfer at data spots," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 3, pp. 37–39, 2010.
15. Xinzhou Wu; Tavildar, S.; Shakkottai, S.; Richardson, T.; Junyi Li; Laroia, R.; Jovicic, A., "Flash LinQ: A Synchronous Distributed Scheduler for Peer-to-Peer Ad-Hoc Networks," *Networking, IEEE/ACM Transactions on , vol. 21, no.4, pp.1215, 1228, 2013.*
16. Ying-Dar Lin; Yu-Ching Hsu, "Multihop cellular: a new architecture for wireless communications," *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies., vol.3, no., pp.1273,1282 vol.3, 26-30, 2000*
17. T. Han and N. Ansari, "On greening cellular networks via multicell cooperation," *IEEE Wireless Communication Magazine., vol. 20, no. 1, pp. 82–89, 2013.*
18. Luo Junhai and Ye Danxia, "A survey of multicast routing protocols for Mobile ad-hoc networks" *IEEE Communication surveys & Tutorials, vol.11, no.1, pp.78-90, 2009.*
19. Luo Junhai, Xue Liu, Ye Danxia, "Research on multicast routing protocols for mobile ad-hoc networks", *Computer Networks vol. 20, no. 1, pp. 988-997, 2008.*
20. Li Layuan "A QoS multicast routing protocol for clustering mobilie ad hoc network" *Computer Communication, 1641-1654. International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010*
21. J. H. Cui and L.Lao. AQoSM: Scalable QoS multicast provisioning in Diff-Serv networks, *Computer Networks 80-105, 2005*.
22. Huayi Wu and Xiaohua Jia "QoS multicast routing by using multiple paths/tress in wireless ad hoc networks", *Ad Hoc Networks 600-612, 2007*.
23. S. S. Manvi, M. S. Kakkasageri, Multicast routing in mobile ad hoc networks by using a multiagent system. *Inf. Sci. 178(6): 1611-1628, 2008.*
24. B.Han, P.Hui, V.A.Kumar,M.V.Marathe, G.Pei andA. Srinivasan,"Cellulartrafficoffloadingthroughopportunisticcommunications: A case study," *5th ACM Workshop Challenged Network.pp. 31–38. 2010.*
25. A. Mashhadi and P.Hui, "Proactive Caching for Hybrid Urban mobile Networks",*http: //www.cs.ucl.ac.uk/research//documents/RN_10_05_000.pdf.*
26. X. Zhuo, W. Gao, G. Cao, and Y. Dai, "Win-coupon: An incentiveframework for 3G traffic offloading," *IEEE International Conference Network Protocols (ICNP),vol 20, no. 1 pp. 206–215.2011.*
27. I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communication. Magazine,* vol 43, no. 9, pp. S23-S30, 2005.
28. N. Li, J. C. Hou, and L. Sha, "Design and analysis of an MST-based topology control algorithm," *IEEE Transaction. Wireless Communication,* vol. 4, no. 3, pp. 1195-1206, 2005.
29. D.-N. Yang, W. Liao, and C.-J. Kao, "Source filtering in IP multicast routing," *IEEE Transaction Broadcasting*, vol. 52, no. 4, pp. 529-542, 2006.
30. D. S. Lun, N. Ratnakar, M. Medard, Ralf Koetter, David R. Karger, Tracey Ho, Ebad Ahmed, and Fang Zhao, "Minimum-cost multicast over coded packet networks," *IEEE Transaction Information Theory*, vol. 52, no. 6, 2006.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350