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

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Web Content Miner
- Virtual Private Network
- Investigation of Botnet
- Wireless Sensor Networks

Discovering Thoughts, Inventing Future

VOLUME 13 ISSUE 9 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 13 Issue 9 (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 Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141 United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU United Kingdom.

Packaging & Continental Dispatching

Global Journals, 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: *investers@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)

Editorial Board Members (HON.)

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 Volume

i. Copyright Notice
ii. Editorial Board Members
iii. Chief Author and Dean
iv. Table of Contents
v. From the Chief Editor's Desk
vi. Research and Review Papers

1. Design of H∞ Congestion Controller for TCP Networks Based on LMI Formulation. *1-7*
2. A Critical Investigation of Botnet. *9-11*
3. A Usability Assessment of Pakistani Universities/Institutions Websites. *13-19*
4. An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme. *21-33*
5. Design and Implementation of Mobility for Virtual Private Network Users. *35-39*
6. Increase the Alive Nodes Based on the Cluster Head Selection Algorithm for Heterogeneous Wireless Sensor Networks. *41-46*

vii. Auxiliary Memberships
viii. Process of Submission of Research Paper
ix. Preferred Author Guidelines
x. Index

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Design of H_∞ Congestion Controller for TCP Networks Based on LMI Formulation

By Aakanksha Shirbhate
Lovely Professional University, India

Abstract - In this paper, a state feedback H_∞ controller has been proposed in order to design an active queue management (AQM) system based on congestion control algorithm for networks supporting TCP protocols. In this approach, the available link bandwidth is modeled as a time-variant disturbance. The objective of this paper is to design controller which capable of achieving the queue size and guarantee asymptotic stability in the present of disturbance. An important feature of the proposed approach is that the performance of system, including the disturbance rejection and stability of closed-loop system, are guaranteed for all round-trip times that are less than a known value. The controller design is formulated in the form of some linear matrix inequalities, which can efficiently solved numerically. The simulation results demonstrate the effectiveness of proposed methods in comparison with other conventional methods.

Indexterms : *TCP, AQM, time delay, H_∞, LMI, stability, disturbance rejection.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Design of H_∞ Congestion Controller for TCP Networks Based on LMI Formulation

Aakanksha Shirbhate

Abstract - In this paper, a state feedback H_∞ controller has been proposed in order to design an active queue management (AQM) system based on congestion control algorithm for networks supporting TCP protocols. In this approach, the available link bandwidth is modeled as a time-variant disturbance. The objective of this paper is to design controller which capable of achieving the queue size and guarantee asymptotic stability in the present of disturbance. An important feature of the proposed approach is that the performance of system, including the disturbance rejection and stability of closed-loop system, are guaranteed for all round-trip times that are less than a known value. The controller design is formulated in the form of some linear matrix inequalities, which can efficiently solved numerically. The simulation results demonstrate the effectiveness of proposed methods in comparison with other conventional methods.

Indexterms : TCP, AQM, time delay, H_∞, LMI, stability, disturbance rejection.

I. Introduction

Communication networks are an essential part of many applications in science and engineering, such as Web servers, multimedia, and remote control. However, traffic congestion is a major problem in today's Internet, because the quality of service cannot be guaranteed, since the number of users has grown rapidly and also unanticipated interference may occur. Therefore, congestion control techniques monitor network loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion control is achieved through packet dropping.

Active queue management (AQM) [1, 2] is a key congestion control scheme for reducing packet drops and improving network utilization. The random early detection (RED) [3] algorithm is the earliest well-known AQM scheme that eliminates the flow synchronization problem and attenuates the traffic load. Unfortunately, RED causes oscillations and instability due to the parameter variations. Therefore, some modified RED schemes, such as FRED [4] and SRED [5], have been proposed in the literature. However in those studies, both high network utilization and low packet loss cannot be guaranteed by only setting control parameters. Recently, control theory has been widely applied to the analysis and design of TCP networks and congestion control schemes for them. In [6], the theory of stochastic equations has been applied to develop a fluid-based model of the dynamics of the TCP and RED. Based on this TCP model, the fundamentals of control theory have been used to analyze and develop new AQM schemes. Proportional-integral (PI) controller was developed for a linearized system and implemented using differential equations [7]. In [8], a sliding mode variable structure control (SMVS) scheme for TCP congestion control has been developed. In [9], proportional-integral-derivative (PID) controllers have been proposed to improve the performance of TCP systems.

While great progress has been made in new congestion control schemes, some problems are still not sufficiently addressed. One important problem is the robustness of the congestion control algorithm against the disturbance on the available link bandwidth since it is often time-varying and cannot be exactly measured.

In this paper a H_∞ state feedback control approach has been proposed. The main difference between our approach and the previous studies [10, 11, 12] is that, the approach proposed here uses a time-domain H_∞ design method, which can deal with the situation where the round-trip time varies with time, while the previous studies use frequency-domain design method, which require that the system under consideration is time invariant.

Structure of the paper is as follows. In section II, system model and problem statement will be presented. We formulate our problem as proposed in [13]. In section III, we discuss how to deal with linear time delay systems. In the next section, a H_∞ state feedback controller is employed to solve the problem for linear time varying systems. In section IV, performance of the closed loop system by using the proposed controller has been discussed in the form of some simulations and the paper is concluded in the section V.

II. Model of the System

We begin our discussion of AQM by introducing a dynamic model for TCP's congestion control.

In [6], a dynamic model of TCP behavior was developed by using fluid-flow and stochastic differential equation analysis. Similar to [13], here a simplified version of that model is used which neglects the TCP timeout mechanism. This model is described by the following coupled and nonlinear delay-differential equations:

Author : Student, Lovely Professional University, Phagwara, Punjab, India. E-mail : aakanksha.artindia@gmail.com

$$\begin{cases} \dot{W} = \dfrac{1}{\tau(t)} - \dfrac{W(t)}{2}\dfrac{W(t-\tau(t))}{\tau(t-\tau(t))}p(t-\tau(t)), \\ \dot{q}(t) = \begin{cases} -C(t) + \dfrac{N(t)}{\tau(t)}W(t), & q(t) > 0, \\ \max\left\{0, -C(t) + \dfrac{N(t)}{\tau(t)}W(t)\right\}, & q(t) = 0 \end{cases} \\ \tau(t) = \dfrac{q(t)}{C(t)} + T_p, \end{cases} \quad (1)$$

Where W is the TCP window size (in packets), q the queue length in the router (in packets), τ the round-trip time (in Sec), C the available link capacity (in packets/s), T_p propagation delay (in Sec.), N the number of TCP sessions, and p the probability of packet mark.

It is assumed that $q \in [0, \bar{q}]$ and $W \in [0, \overline{W}]$, where $\bar{q}$ and $\overline{W}$ denote buffer capacity and maximum window size, respectively. The marking probability p belongs to the interval [0, 1]. In practical networks, the available link capacity changes with time and it is difficult to measure. Therefore it is taken as a disturbance in a lot of studies [14, 15, 16]. In this paper, it is supposed that the nominal value of $C(t)$, say C_0, is known, while $\delta C(t) \triangleq C(t) - C_0$ is unknown and considered as a disturbance for the system.

Take (W, q) as the states and p as the input of the system. For a given triplet of network parameters (N, C_0, T_p), any triplet (W_0, q_0, p_0) that is in the set

$$\Omega = \{(W_0, q_0, p_0) : W_0 \in [0, \overline{W}], q_0 \in [0, \bar{q}], p_0 \in$$

$$[0,1],\ \tau_0 = \frac{q_0}{C_0} + T_p,\ W_0 = \frac{\tau_0 C_0}{N},\ p_0 = \frac{2}{W_0^2}\}$$

is a possible operating point. Now define

$$\delta W = W - W_0, \quad \delta q = q - q_0, \quad \delta p = p - p_0, \quad \delta C = C - C_0.$$

We can obtain the linearized version of (1) as follows

$$\begin{cases} \delta\dot{W} = -\dfrac{N}{\tau_0^2 C_0}\left[\delta W(t) + \delta W(t-\tau_0)\right] \\ \quad -\dfrac{1}{\tau_0^2 C_0}\left[\delta q(t-\tau_0)\right] \\ \quad -\dfrac{\tau_0 C_0^2}{2N^2}\delta p(t-\tau_0) + \dfrac{\tau_0 - T_p}{\tau_0^2 C_0}\left[\delta C(t) - \delta C(t-\tau_0)\right], \\ \delta\dot{q} = \dfrac{N}{\tau_0}\delta W(t) - \dfrac{1}{\tau_0}\delta q(t) - \dfrac{T_P}{\tau_0}\delta C(t). \end{cases} \quad (2)$$

In contrast to the case of linear systems without delay, the solution for the H_∞ control problem for time delay systems is quite different.

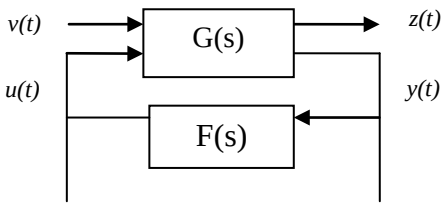


Figure 1 : A general setting for the H_∞ control design

When the delay appears only in the state variables, there are lots of results like [17, 18]. But for the case where the time delay also appears in control variables, there is not any obvious solution.

The objective of this paper is to develop a H_∞ design approach for the problem of AQM-based congestion control based on the dynamic model (2), which guarantees the ratio between the norms of some desired variables and that of the disturbance being less than some specified value. Furthermore, this specified value for the ratio can be minimized for a given group of network parameters. To this end, we will first study the H_∞ control of general linear time delay systems and then apply the result to the above mentioned system.

III. H_∞ Control of Linear Time Delay Systems

As is well-known, the primary goal of a control algorithm is to guarantee that the closed-loop system is stable. For linear time-invariant single-input-single-output (SISO) plant without delay, this goal can be easily achieved by using classical controller design approaches, developed in 1950s and 1960s. Furthermore, the gain and phase margin indicated in these classical approaches provide a good measure for the robustness of closed-loop systems. However, it is difficult to apply these approaches to the controller design of a multi-input-multi-output (MIMO) plant or a time delay system. On the other hand, dealing with model uncertainty and disturbance is a main concern of control engineers. Therefore, various robust controller design approaches for complex plants have been developed since the 1980s. The H_∞ design is one of those approaches.

A general setting for the H_∞ design is illustrated in Fig. 1, where u is a control input, v the exogenous disturbance, z is the controlled output, and y is the measured output. The controlled output means the variable we want to regulate by designing a controller F. The objective of the H_∞ control design is to find a controller F such that

$$\|F_{zv}\| \le \gamma \quad (3)$$

Clearly, γ describes a kind of disturbance rejection ratio between the controlled variable and the exogenous disturbance.

Comparing system (2) to Fig. 1, and setting, $z(t)=q(t),\ v(t)=\delta C,$ It can be seen that, under a H_∞ control scheme, the queue length of the router will be maintained level, which is implied by the asymptotical stability of the system, with minimum sensitivity to the fluctuation of the available link bandwidth, which is implied by the minimum of the disturbance rejection ratio. Therefore, it is a nature desire to develop a H_∞ design approach to the congestion control problem. Now consider the following system

$$\begin{aligned}\dot{x}(t) &= A_0x(t)+A_1x(t-\tau(t))+B_0u(t)+B_1u(t-\tau(t))+D\upsilon(t),\\ z(t) &= Hx(t),\end{aligned} \tag{4}$$

Where $x(t)\in\Re^n$ is the system state, $u(t)\in\Re^{n_u}$ the control input, $\upsilon\in\Re^n$ the exogenous disturbance, $z\in\Re^{n_z}$ the controlled output, and τ the time-delay involved. Suppose that τ is upper-bounded by $\tau_m : 0\le\tau\le\tau_m$. All matrices are of appropriate dimensions. Throughout this section, it is defined that $A=A_0+A_1$ and $B=B_0+B_1$.

For a prescribed scalar $\gamma>0$, define the performance index as

$$J(\gamma)=\int_0^\infty (Z^T(t)z(t)-\gamma^2\upsilon^T(t)\upsilon(t))dt. \tag{5}$$

The objective is to find a control law of the type $u(t)=Kx(t)$ such that the closed-loop system satisfies $J(\gamma)<0$ for any $\upsilon\in L_2^{n_\upsilon}[0,\infty)$. Furthermore, minimize γ if possible. Note that the requirement $J(\gamma)<0$ means that

$$\frac{\|z\|}{\|\upsilon\|}=\frac{\sqrt{\int_0^\infty z^T(t)z(t)dt}}{\sqrt{\int_0^\infty \upsilon^T(t)\upsilon t)\upsilon(t}}<\gamma \tag{6}$$

Where $\|.\|$ refers to the 2-norm in the space $L_2^{n_\upsilon}[0,\infty)$. Eq. (6) says that the ratio between the norm of the controlled output and that of the disturbance is less than a specified scalar γ.

To solve the above problem, the bounded real lemma (BRL) for time delay systems is needed. Up to now, several versions of BRL have been reported [19, 20], we use formulation of [19] to solve the problem.

Lemma 1 :

Consider system (4) with $u(t)\equiv 0$. If there exist matrices $R>0$ and $P\triangleq\begin{bmatrix}P_1 & 0\\ P_2 & P_3\end{bmatrix}$ with $P_1>0$ such that the following linear matrix inequality (LMI).

$$\begin{bmatrix} P^T\begin{bmatrix}0 & 1\\ A & -1\end{bmatrix}+\begin{bmatrix}0 & A^T\\ 1 & -1\end{bmatrix}P+\begin{bmatrix}H^TH & 0\\ 0 & \tau_mR\end{bmatrix} & P^T\begin{bmatrix}0\\ D\end{bmatrix} & \tau_mP^T\begin{bmatrix}0\\ A_1\end{bmatrix}\\ [0\quad D^T]p & -\gamma^2I & 0\\ \tau_m[0\quad A_1^T]p & 0 & -\tau_mR\end{bmatrix}<0 \tag{7}$$

holds, then system (3) achieves $J(\gamma)<0$.

Based upon Lemma 1, the following theorem can be established.

Theorem 1 :

Consider system (4). If there exist matrices $Q_1>0$, Q_2, Q_3, Y and positive scalar ε such that the matrix inequality (11) holds, then the closed-loop system achieves $J(\gamma)<0$ with the controller

$$u(t)=Kx(t),\quad K=YQ_1^{-1}. \tag{8}$$

Remark 1 :

From Theorem 1, we can see an interesting feature of the approach: the system performances, including the disturbance rejection ratio γ and the implied stability of the closed-loop system, are guaranteed for all time delay that is less than τ_m. This feature is especially important for the congestion control problem since the round-trip time is actually state-dependent and hence time-varying, whereas its upper bound can be roughly estimated.

In congestion control, one important problem is to find maximum allowable upper bound of the time delay such that the network can still be stabilized or a H_∞ performance index can still be guaranteed. This problem can be easily dealt based on the following corollary.

Corollary 1 :

Consider system (4). For a given positive scalar γ, if there exist matrices $Q_1>0$, $\overline{Q_1}>0$, Q_2, Q_3, Q_4 and positive number ε such that the following matrix in equalities

$$\begin{bmatrix}\psi_2 & \eta_1 & \eta_2\\ \eta_1^T & -\varepsilon\overline{Q_1} & 0\\ \eta_2^T & 0 & -\frac{1}{\varepsilon}\overline{Q_1}\end{bmatrix}<0 \tag{9}$$

$$\overline{Q_1}<\frac{1}{\tau_m}Q_1 \tag{10}$$

hold, where

$$\psi_2 = \begin{bmatrix} Q_2 + Q_2^T & Q_1A^T + Y^TB^T - Q_2^T + Q_3 & 0 & Q_1H^T \\ AQ_1 + BY - Q_2 + Q_3^T & -Q_3 - Q_3^T & D & 0 \\ 0 & D^T & -\gamma^2 I & 0 \\ HQ_1 & 0 & 0 & -I \end{bmatrix}$$

$$\begin{bmatrix} Q_2 + Q_2^T & Q_1A^T + Y^TB^T - Q_2^T + Q_3 & 0 & 0 & Q_1H^T & Q_2^T \\ AQ_1 + BY - Q_2 + Q_3^T & -Q_3 - Q_3^T & D & \tau_m(A_1Q_1 + B_1Y) & 0 & Q_3^T \\ 0 & D^T & -\gamma^2 I & 0 & 0 & 0 \\ 0 & \tau_m(Q_1A_1^T + Y^TB_1^T) & 0 & -\tau_m\varepsilon Q_1 & 0 & 0 \\ HQ_1 & 0 & 0 & 0 & -I & 0 \\ Q_2 & Q_3 & 0 & 0 & 0 & -\dfrac{1}{\tau_m\varepsilon}Q_1 \end{bmatrix} < 0 \quad (11)$$

$\eta_1 = [0 \quad (A_1Q_1 + B_1Y)^T \quad 0 \quad 0]^T$, $\eta_2 = [Q_2 \quad Q_3 \quad 0 \quad 0]^T$ then the closed-loop system achieves $J(\gamma) < 0$ with the controller $u(t) = Kx(t), \quad K = YQ_1^{-1}$.

Furthermore, parameter τ_m can be maximized by solving the generalized Eigen value problem defined by (9) and (10). It can give us the maximum allowable time delay for the system that closed loop system can be stable yet.

IV. H_∞ Controller Performance

In this section, the result obtained in the former section will be applied to the RED-based congestion control problem.

The short-lived http flows are introduced into the router and modeled with δC as a birth-and-death process. Specifically, construct δC as:

$$\delta C = B_{av}k(t)$$

Where $k(t)$ is a birth-and-death process with the birth and death rates being λ and μ, respectively, and B_{av} is the average transmission rate of http flows. According to [21], it is appropriate to use a birth-and-death process to model http flows. Note that the value of the available link capacity at the equilibrium may be also over-estimated, so δC might take negative values too. Considering this fact, $k(t)$ is allowed to take negative values. It is natural to assume that the birth rate and death rates are equal. Thus such a process is null-recurrent, i.e., the process does not keep visiting any state frequently. Therefore, gain $k(t)$ will diverge inevitably. Obviously, this does not match the practical situation. To remedy it, we place lower and upper bounds for $k(t)$, namely $-k_{\max} \le k(t) \le k_{\max}$, where $k_{\max}$ is a positive number. Thus $k(t)$ can be viewed as a modified birth-and-death process with lower and upper barriers. This is realized in simulation by simply removing the constraint $k \ge 0$ in the original model of the birth_death process and placing the new constraint $-k_{\max} \le k(t) \le k_{\max}$ on it.

Note that in model (2), the delayed version of the exogenous disturbance also appears in the dynamics of the system. To take into account of this fact, define

$$\bar{\upsilon}(t) = [\delta C(t) \quad \delta C(t - \tau_0)]^T$$

and change the objective function for H_∞ control design as

$$\bar{J}(\gamma) = \int_0^\infty (z^T(t)z(t) - \gamma^2\bar{\upsilon}^T(t)\bar{\upsilon}(t))dt.$$

It is clear that the performance $J(\gamma) < 0$ is satisfied if the closed-loop system achieves $\bar{J}(\gamma) < 0$.

Associating model (2) with the general system model (4), we can extract A_0, A_1, B_0, B_1, D matrices. The matrix H is chosen as $H = [0 \quad 1]$ for all cases to be studied. The approach proposed here is compared with the performance of P and PI controllers in [13]. Therefore, constant parameters of model extract from [13]. Where C=3750 packets/s, N=60 flows and τ_0 *=0.246 Sec.*

$$x(t) = \begin{bmatrix} \delta W(t) \\ \delta q(t) \end{bmatrix},$$

$$A_0 = \begin{bmatrix} -\dfrac{N}{\tau_0^2 C_0} & \dfrac{1}{\tau_0^2 C_0} \\ \dfrac{N}{\tau_0} & \dfrac{1}{\tau_0} \end{bmatrix}, \qquad A_1 = \begin{bmatrix} -\dfrac{N}{\tau_0^2 C_0} & -\dfrac{1}{\tau_0^2 C_0} \\ 0 & 0 \end{bmatrix},$$

$$B_0 = 0, \qquad B_1 = \begin{bmatrix} -\dfrac{\tau_0 {C_0}^2}{2N^2} \\ 0 \end{bmatrix} \qquad D = \begin{bmatrix} \dfrac{\tau_0 - T_P}{\tau_0^2 C_0} & -\dfrac{\tau_0 - T_P}{\tau_0^2 C_0} \\ \dfrac{T_p}{\tau_0} & 0 \end{bmatrix}$$

By substitution of the constant parameters in the above matrices, we have the following results:

$$A_0 = \begin{bmatrix} -0.2644 & -0.0044 \\ 243.9024 & -4.0650 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} -0.2644 & 0.0044 \\ 0 & 0 \end{bmatrix},$$

$$B_0 = 0$$

$$B_1 = \begin{bmatrix} -480.4688 \\ 0 \end{bmatrix}$$

$$D = \begin{bmatrix} 2.3487*10\text{^}(-10) & -2.3487*10\text{^}(-10) \\ -0.7833 & 0 \end{bmatrix}$$

In this case the PI controller has a transfer function

$$C(s) = K_{PI} \frac{(\frac{s}{z}+1)}{s}$$

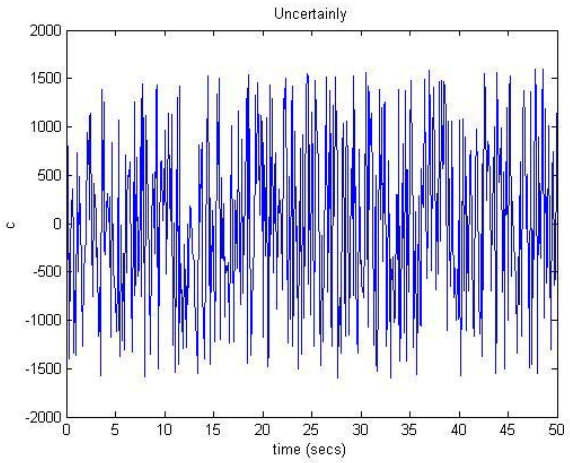


Figure 1 : The disturbance on the available link bandwidth

With $K_{PI} = 9.64 \times 10^{-6}$ and $z = 0.53$. The P controller has transfer function

$$C(s) = K_P$$

With $K_P = 5.8624 \times 10^{-5}$.

For design of H_∞ controller based on LMI formulation, we first use constant parameters to calculate A_0, A_1, B_0, B_1, D matrices. Then we determine the maximum delay which the controller is robust against it. We solve (11) to find the state feedback K as follows:

$$K = [-1.5357e-003 \quad 2.3272e-005]$$

In all simulations, the initial windows size of every source and the initial queue length of the router are set to be zero. For each case controller, the same disturbance profile on the available link bandwidth is used for PI, P and H_∞ controllers.

From Fig. 2, we can see the disturbance on the available link bandwidth which is the result of birth and death process with $B_{av} = 32$ and $k_{\max} = 50$.

From Fig. 3 and 4, we can see that, by using the H_∞ controller, a stable operating condition can be built up and maintained even in the situations where the available link bandwidth is subjected to presence of disturbance and the round-trip varies with different TCP sessions, while PI controller fail to do so. This is due to the lag of the response of the conventional PI controller to the sudden change of the network operating condition.

The responses of the queue size for the duration of time from 0 to 5 s can be observed in Fig. 3 and 4 respectively. It is clear that both H_∞ and P controllers yield lower overshoot than PI, and yield almost bigger rise time than PI. Also from Table 1, it is obvious that the maximum overshoot in H_∞ is smaller than P and PI controllers in both queue length and window size states.

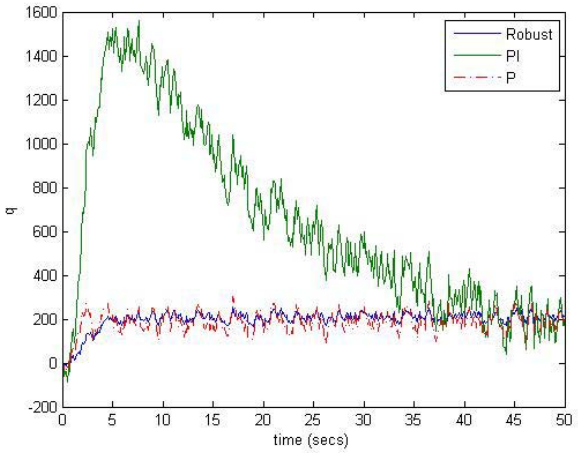


Figure 2 : Queue length responses using H_∞, P and PI controllers

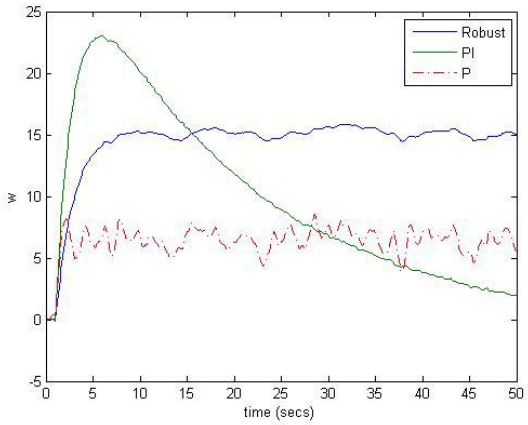


Figure 3 : Window size responses using H_∞ , P and PI controllers

Table 1 : Compare performance of H ∞, PI and P controllers

Characteristics	H∞	PI	P
Queue length maximum overshoot	6.6%	50%	40%
Window size maximum overshoot	25%	67.5%	50%

V. Conclusion

In this paper, a new design method for the H_∞ congestion controller of the TCP has been developed based on the LMI technique. In the approach, the available link bandwidth is modeled as a nominal constant value, which is known to the link, plus a time-variant disturbance, which is unknown.

The proposed approach can theoretically guarantee the system performance, including the disturbance rejection and the implied stability of the closed-loop system for all round-trip times that are less than a known value. Finally, it is pointed out that the effectiveness of the proposed approach has been verified only via simulation in Matlab. Further verification via packet-based simulation tools such as NS2 or via experimental studies is needed.

References Références Referencias

1. Floyd S, Jacobson V., "Random early detection gateways for congestion avoidance", IEEE/ACM Transactions on Networking, 1997, pp. 1–22.
2. Clark DD, Fang W., "Explicit allocation of best effort packet delivery service", IEEE/ACM Transactions on Networking , 1998, 362–73.
3. Branden B, Clark D, Crowcroft J., "Recommend-ations on queue management and congestion avoidance in the internet", RFC2309. 1994.
4. D. Lin, R. Morris, "Dynamics of random early detection", Proceedings of the ACM SIGCOM'97, Cannes, 1997, pp. 127–137.
5. T.J. Qtt, T.V. Lakshman, L.H. Wong, "SRED: Stabilized RED", Proceedings of the IEEE INFOCOM'99, New York, 1999, pp. 1346–1355.
6. V. Misra, W.B. Gong, D. Towsley, "Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to RED", Proceedings of the ACM/SIGCOM, Stockholm, 2000, pp. 151–160.
7. C.V. Hollot, V. Misra, D. Towsley, W.B. Gong, "On designing improved controllers for AQM routers supporting TCP flows", Proceedings of the IEEE INFOCOM, Alaska, USA, 2001, pp. 1726–1734.
8. F.Y. Ren, C. Lin, X.H. Yin, "Design a congestion controller based on sliding mode variable structure control", Computer Communications, 2005, pp. 1050–1061.
9. Kim KB, "Design of feedback controls supporting TCP based on the state-space approach", IEEE Transactions on Automatic Control 2006, pp. 1086–99.
10. Quet, P.F., Özbay, H., "On the design of AQM supporting TCP flows using robust control theory", IEEE Transactions on Automatic Control, 2004, 49, 1031-1036.
11. Chen, Q., & Yang, O. W., "Design of AQM controller for IP routers based on H1 S/U MSP", IEEE intern. conf. on communications, 2005, pp. 340-344.
12. Chen, Q., & Yang, O. W., "Robust controller design for AQM router", IEEE Transactions on Automatic Control, 2007, pp. 938-943.
13. Hollot, C. V., Misra, V., Towsley, D., & Gong, W. B., "Analysis and design of controllers for AQM routers supporting TCP flows", IEEE Transactions on Automatic Control, 2002, pp. 945-959.
14. Cavendish, D., Gerla, M., & Mascolo, S., "A control theoretical approach to congestion control in packet networks", IEEE/ACM Transactions on Networking, 2004, pp. 893-906.
15. Fan, X., Arcak, M., & Wen, J. T., "Robustness of network flow control against disturbances and time-delay", Systems Control Letters, 2004, pp. 13-29.
16. Mascolo, S., "Congestion control in high-speed communication networks using the Smith principle", Automatica, 1999, pp. 1921-1935.
17. Lee, Y. S., Kwon, W. H., & Park, P. G., "Authors reply: Comments on delay-dependent robust H1 control for uncertain systems with a state-delay", Automatica, 2007, pp. 572-573.
18. Yang, F., Wang, Z., Hung, Y. S., & Gani, M., "H1 control for networked systems with random communication delays", IEEE Transactions on Automatic Control, 2006, pp. 511-518.
19. Fridman, E.,&Shaked, U., "New bounded real lemma representations for timedelay systems and their applications", IEEE Transactions on Automatic Control, 2001, pp. 1973-1979.

20. Shaked, U., Yaesh, I., & de Souza, C., "Bounded real criteria for linear timedelay systems", IEEE Transactions on Automatic Control, 1998, pp. 1016-1022.
21. Bertsekas, D., & Gallager, R. G., "Data networks", Upper Saddle River, NJ: Prentice-Hall, 1992.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Critical Investigation of Botnet

By Rathod R.P., Bhalchandra P.U., Dr. Khamitkar S.D & Lokhande S.N.
SRTM University's Sub Center, Latur (MS), India

Abstract - A Botnet is a network of compromised hosts, called as bots that are used for malicious activity. These bots are then controlled by single master termed as Botmaster. A Botmaster may inject commands though any bot to launch DDoS attack. In this paper, we have demonstrated the behavior of Botnet on network in real time Internet environment.This will be helpful for researcher to detect the different types of emerging Botnet.

Keywords : *network security, botnet, denial of service attack.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

A Critical Investigation of Botnet

Rathod R.P. [α], Bhalchandra P.U. [σ], Dr. Khamitkar S.D [ρ] & Lokhande S.N. [ω]

Abstract - A Botnet is a network of compromised hosts, called as bots that are used for malicious activity. These bots are then controlled by single master termed as Botmaster. A Botmaster may inject commands though any bot to launch DDoS attack. In this paper, we have demonstrated the behavior of Botnet on network in real time Internet environment. This will be helpful for researcher to detect the different types of emerging Botnet.

Keywords : network security, botnet, denial of service attack.

I. Introduction

A Botnet is large group of compromised hosts known as bots. Symantec [1] defines a bot as "Bots are similar to worms and Trojans, but earn their unique name by performing a wide variety of automated tasks on behalf of their master". The bots are also known as zombies. . The Botnet are used for different attacks such as DDoS, spamming, phishing, sniffing, etc. These bots are controlled by a Botmaster through the command & control (C&C) mechanism as shown in figure 1. Based on this C&C mechanism Botnet can classified into IRC, P2P and HTTP Botnet.

II. Command & Control (C&C) Mechanism

The Botmaster uses the C&C mechanism to control the bots .This mechanism states the how Botmaster to assign the commands to the bots. The C&C mechanism classified into centralized, P2P, IRC, and HTTP.

a) Centralized

This is the most widely used mechanism by the Botmaster. In this mechanism, a central server is used communication with bots. The commands are downloaded by the bots known as pull or sent to bots known as push. In push style the bots directly controlled by the Botmaster. While, in case of pull style Botmaster does not have direct control bot has to received the commands by interacting with C&C server periodically [2]. The IRC and HTTP protocols are widely used by this mechanism.

b) P2P Mechanism

As the name implies there is no central server. The bot acts as client and server to form Botnet; hence the detection is harder compared to other Botnet. If one bot is removed still other bots continue the communication which gives more flexibility for Botnet.

Author α : SRTM University's Sub center, Latur (MS), India.
E-mail : srtmun.parag@gmail.com
Authors σ ρ ω : School of Computational Sciences, SRTM University, Nanded, MS, India.

c) IRC (Internet Relay Chat)

This is the most popular and old mechanism used by the Botnet. The bots are connected to IRC server using IRC protocol. Bots communicates though push mechanism and they chats with each other with the help of commands.

d) HTTP

Here the commands are not sent directly to the bots, instead it leaves malicious program on a web server and bot uses the pull mechanism for commands.

III. Botnet Existence Phases

a) Preliminary Infection and Transmission

Botnet are formed though a vulnerable hosts. The Botmaster gain the access of infected host using different techniques such as operating system or application vulnerability. The Botmaster also uses the websites, emails as a spreading channel. When the user click on website link of opens an email the bot get installed on a victim's machine and become part of Botnet. [3]

b) C&C Server Actions

When the bot get installed on the Botmaster uses the pull or push methods for communication with bots. The C& C server controls the bots though IRC channel. The bot get connected to IRC server with a nickname and then it join to Botnet.

c) Accepting Instructions

When the bot joins the IRC Server Botmaster sends instructions to the bots. These instructions include commands which are used for various malicious activities or attacks.

d) Disseminations using other hosts

The Botnet spread though the vulnerable hosts, so the Botmaster uses C&C server to search such a host to become a part of Botnet.

IV. Case Study: IRC Botnet

IRC Botnet is the most popular Botnet which uses the centralized mechanism to control the bots. This Botnet uses the IRC channel for communication and controlling the bots. We have tested in a secure environment to avoid infection to other unwanted hosts.

We have used a bot which performs different tasks and attacks such as port scanning, port scanning, UDP flood, TCP flood, http flood, SQL flood etc.

When the bot connect to IRC server he/she joins the channel where other users are already login by nicknames. When a user submits the messages to IRC server publically the other user can see her/his messages on the channel [4]. IRC include list of channels a user can join any channel though an IRC chat client by channel name.

IRC server commonly uses the port 6667 where user gets joined to IRC server. The channel administrator handles all the users. The user can use the commands as follows:

1. JOIN: Joins a channel
2. PASS: set or send a password
3. QUIT: Exit a channel
4. SEND: Send the file to another IRC user
5. RAW : Will do the raw scan
6. JUMP: Jump to another IRC server
7. QUIT: Quit the channel

a) Experiment Setup

Our experiment consists of one IRC server hosted on cloud server with Ubuntu 12.04 and two dummy servers working as bot all are connected in real time Internet environment as shown in following figure 1. We have installed packet capturing tool 'tcpdump' on these servers. The client is installed with Xchat software for joining the channels on IRC server.

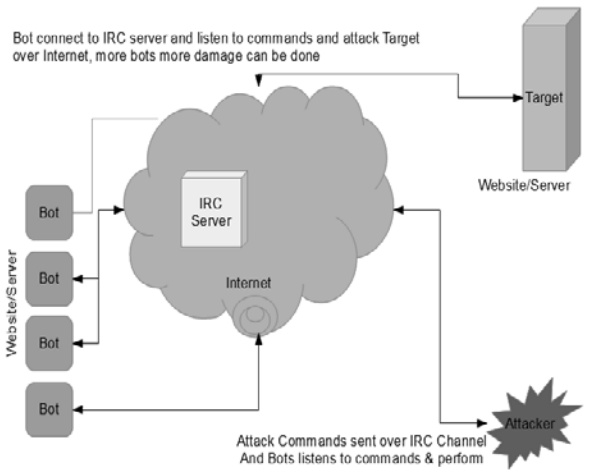


Figure 1 : Experimental Setup for Botnet Attacks

When the user joins a channel on IRC server, he/she become the channel operator. When the bot is setup on victim's machine from IRC server, the Botmaster tries to hide it's identity from IRC Server by using node commands [4]. The user joins the channel by using user name. First we have collected the network traffic with the help of 'tcpdump' and then converted to CSV for further analysis.

We have tested the bot to obtain the actual working of bot and Botmaster. In this experiment bots are controlled by using the commands and launch

We have tested the bot to obtain the actual working of bot and Botmaster. In this experiment bots are controlled by using the commands and launch different attacks. The network traffic contains traffic from IRC to bot and other hosts in the network.

b) Flow Characteristics

Our experiment contains over 260000 packets with the flow characteristics shown in below table1. We have filtered this traffic to separate normal or legitimate and Botnet traffic. During the experiment the protocol hierarchy statistics is shown in the following table 2.

Name of Field	Filed Details
Source	Source IP address
Destination	Destination IP address
Protocol	Name of protocol
Length	Packet Length in bytes
Info	Information about packet

Table 1 : Flow Characteristics

Protocol	% Packets	Packets
Transmission Control Protocol	54.1 %	142640
SSH Protocol	0.10 %	270
Internet Relay Chat	7.50 %	19748
Virtual Router Redundancy Protocol	4.75 %	12524
User Datagram Protocol	7.38 %	19443
Domain Name Service	5.10 %	13441
Drop box LAN sync Discovery Protocol	0.58 %	1534
NetBIOS Name Service	1.43 %	3766
Internet Control Message Protocol	0.02 %	45
IP v6	0.01 %	33
SMB	0.18 %	462
Internet Group Management Protocol	0.16 %	415
Address Resolution Protocol	29.20 %	76943
Logic-Link Control	2.24 %	5907
Spanning Tree Protocol	2.17 %	5715
Cisco Discovery Protocol	0.07 %	192
IP V6	2.10 %	5545
DHCP V6	1.18 %	3098
Domain Name Service	0.84 %	2208
HTTP	0.03 %	66
ICMP v6	0.07 %	173

Table 2 : Protocol Hierarchy Statistics

c) Bot Communication

When the bot join the channel the Botmaster controls the bot, the captured traffic by Wireshark is shown in following figure 2. The victim joins using port 6667. It is observed that the packet length of Botnet traffic is within the range of 50~500 bytes.

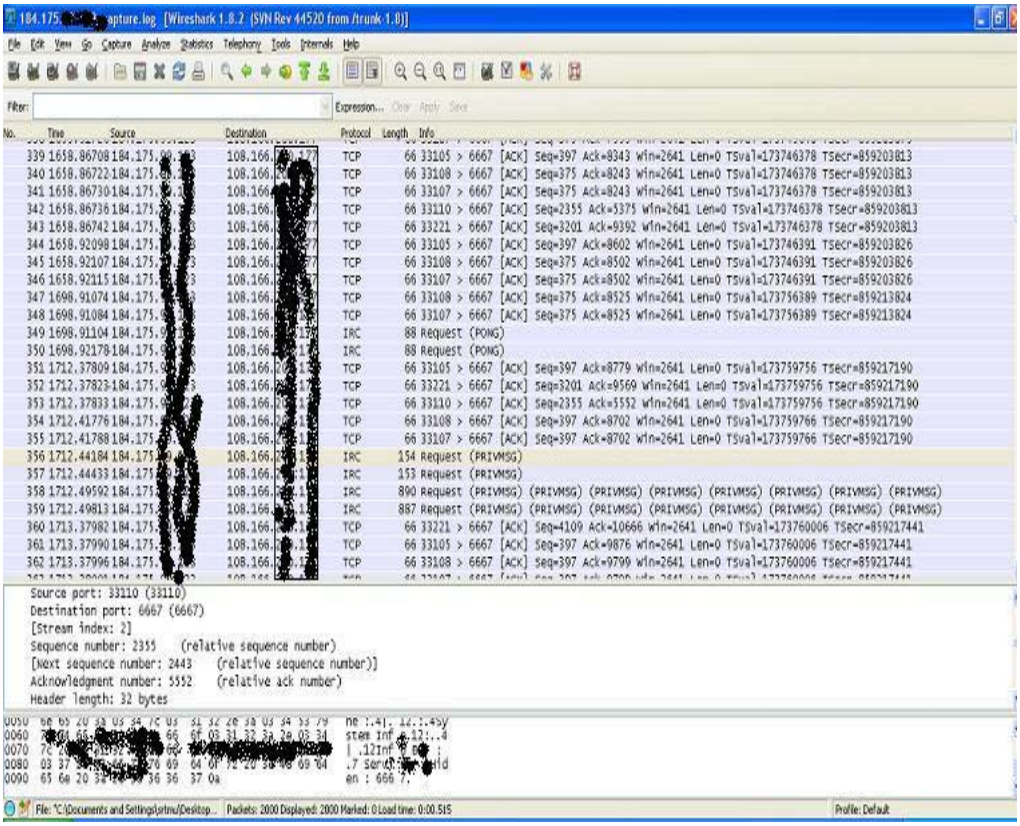


Figure 2 : Result Analysis

V. Conclusion

Botnet are emerging threat with hundreds of millions of computers infected. A study of Zhaosheng Zhu, Northwestern University, USA, shows that about 40% of all computers connected to the internet in the world are infected bots and controlled by attackers. Our paper experimentally shows the behavior and understanding of Botnet attacks. Understanding Botnet, detecting and tracking Botnet, and defending against Botnet is need of time. While Botnet are widespread, the research and solutions for Botnet are still in their infancy.

References Références Referencias

1. Symantec. Crime ware: Bots. http://www.symantec.com/avcenter/cybercrime/bots_page1.html, 2008.
2. Dittrich, D., Dietrich, S.: P2P as Botnet command and control: a deeper insight. Applied Physics Laboratory University of Washington, Computer Science Department Stevens Institute of Technology (2008).
3. S. Racine. Analysis of Internet Relay Chat Usage by DDoS Zombies. Master's Thesis. Swiss Federal Institute of Technology, Zurich. April 2004.
4. M. Overton. Bots and Botnet: Risks, Issues and Prevention. In Proceedings of Virus Bulletin Conference 2005. Dublin, Ireland. October 5-7, 2005.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Usability Assessment of Pakistani Universities/Institutions Websites

By Muhammad Shahid Khan, Naveed Khan, Muhammad Abid Khan & Muhammad Ahmed Javed
Gandhara University, Pakistan

Abstract - Websites are playing a very important role in field of information Technology. Usability is also of much importance in exploring the websites. The objective of this paper is assessing the usability of the websites of the Pakistani Universities and giving the idea of developing the websites of the universities/institutions fulfilling the user needs. Different parameters were analyzed in light of usability in the websites of different universities in Pakistan. It was evaluated that these universities websites have the errors in the parameters not following the rules of usability. The usability of websites of different universities/institutions of Pakistan can be improved applying the one rule for every factor so that the user can encounter every task easily with no tedious effort and confusion. These rules of usability should be announced by the government and the universities should be limited in these rules to facilitate the fresh and experienced users.

GJCST-E Classification : K.4.0

Strictly as per the compliance and regulations of:

A Usability Assessment of Pakistani Universities/Institutions Websites

Muhammad Shahid Khan [α], Naveed Khan [σ], Muhammad Abid Khan [ρ] & Muhammad Ahmed Javed [ω]

Abstract - Websites are playing a very important role in field of information Technology. Usability is also of much importance in exploring the websites. The objective of this paper is assessing the usability of the websites of the Pakistani Universities and giving the idea of developing the websites of the universities/institutions fulfilling the user needs. Different parameters were analyzed in light of usability in the websites of different universities in Pakistan. It was evaluated that these universities websites have the errors in the parameters not following the rules of usability. The usability of websites of different universities/institutions of Pakistan can be improved applying the one rule for every factor so that the user can encounter every task easily with no tedious effort and confusion. These rules of usability should be announced by the government and the universities should be limited in these rules to facilitate the fresh and experienced users.

I. Introduction

Usability is an eminence element that analyzes how the interfaces are easy to use for the user. The following components can easily define the usability [1].

- Learnability is related with encountering the design for the first time; it will be simple for the users to perform the essential tasks.
- Efficiency is how rapidly a user can encounter the different tasks after learning the design.
- Memorability is to which extent the user has the ability to perform different tasks easily which he had encountered few years ago.
- Errors are how many mistakes made by the user, how rigorous they are and how easy they can be recoverable.
- Satisfaction is to what limits the design is satisfying?

Usability has much importance in the web e.g. if the website is designed so that a user is feeling comfortable to accomplish different tasks he wants and he is aware of the current location in the website (where he is in website now), so it is good, otherwise he will be confused and will never visit this website.

a) Logo

On every page, there should be placed a logo of the organization at a constant place (top left corner), so that the user is confident about himself that he is searching the same site to which he has entered some time ago [2].

b) Title

Title/Name should be placed on every page and there should be a link on it [3].

c) Search

On all pages of the website, there should a search option so that the users need not to go to the home page to search the specific word or topic [4].

d) Breadcrumbs

It cannot be expected from the user for using the breadcrumbs efficiently. The competence of the navigation can be increased by using the breadcrumbs in effective way and directions will be provided to the users visiting the website [5].

e) Visited and Unvisited Links

There should be the proper colors for the visited and unvisited links. A link should be of specific color (blue) before it is visited and its color should be changed to another color (purple) to assist the user to notify him the visited and unvisited links [6].

f) Avoid Scrolling Horizontally

There should be a proper layout of the page so that the user can get rid of scrolling horizontally. Scrolling horizontally is the time consuming and boring process for the user for viewing the whole contents of the screen [7].

g) Back button is disabled

Different websites have different links that open the new window and when they are opened by the user, the back button is found disabled and the new opened windows have no information about the past navigation of the user [8].

h) Font Size

The font size in the websites should be at least 12pts [9].The older persons of 65 years age and above are elder (ages 65 and older) are the fastest emergent on the net and 43% older persons face problem as compared to the young persons [10].

i) Typeface

There should be the two font style i.e. Verdana or Arial and the Verdana font style is preferred and is linked on all the pages of the website. This font style can

Author α σ : Gandhara University, Peshawar, Pakistan.
E-mails : shahidkhan123@gmail.com, naveediit@gmail.com
Author ρ : University of Engineering & Technology, Peshawar, Pakistan. E-mail : engrabid08@gmail.com
Author ω : Government Degree College, Kohat, Pakistan.
E-mail : ahmed.javed725@gmail.com

be used in the whole website to increase the efficiency of the website [11].

j) About US

The About us section is visited by the users to know about the university/Institution website to decide about believing him. It has been surveyed that the sites and mission, and decide whether to trust the organization. Our studies show that companies neglect vital prospect to join with users through the portal [12].

k) Site Map

Site maps are used in different websites supplying the summary of the whole website. It provides the tree structure of the website [13].

1. *Quaid E-Azam (http://www.qau.edu.pk/)*

S. No.	Parameters	Yes	No
1	Logo	Yes (But hidden on linked pages)	
2	Title	yes	
3	Search		No
4	Breadcrumbs	yes	
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	yes	
8	Font Size	yes	
9	Typeface	yes	
10	About us used for org. info		No option available
11	Site Map	yes	

In accordance with the different rules and searching for these rules in the website of the above mentioned institution, it has been taken in the consideration.

The monogram of the institution is present on the home page at its proper place (top left corner), but when the website was further navigated, there is missing of the monogram on the top left corner of linked pages. The title of the site is present on the home page as well as on the linked pages at the top of the page but the link is not available on this title.

According to the rules, there should be a search option on the top right side of the page on the home page as well as on the linked pages, but after searching that site, there is no search option on the home page and the linked pages.

The breadcrumbs are creating step by step in the site when this site is further visited.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

As according to the rules, there should be an "About Us" option in which there will be the information about the organization/institution, but after visiting the site of that institution, it has been noticed that there is no "About Us" option present on the page.

The "Site Map" is present on the page of the site which shows all the contents of the site in hierarchy structure, so by clicking on the "Site Map", it will be helpful for the user to see that what contents this site involves.

2. *PIEAS (http://www.pieas.edu.pk/)*

S. No.	Parameters	Yes	No
1	Logo		No
2	Title	yes	Link not available
3	Search		No
4	Breadcrumbs		No
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	yes	
8	Font Size	Yes	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map		No

The monogram of the institution is not at the proper place (top left corner).

The title is available on the home page and on the linked pages but the link is not available on this title.

According to the rules, there should be a search option on the top right side of the page on the home

page as well as on the linked pages, but after searching that site, there is no search option on the home page and the linked pages.

There is no creation of the breadcrumbs when the site is further explored.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far. There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally. When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site. The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

"Site Map" is not present which can lead to confusion for the user because the "Site Map" provides the contents of the website in tree structure from which a user can estimate that what the contents it involves in less time.

3. *Aga Khan University, Karachi (http://www.aku.edu/Pages/home.aspx)*

S#	Parameters	Yes	No
1	Logo	Yes	Not a Top left
2	Title	yes	
3	Search	Yes	
4	Breadcrumbs	Yes	
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	Yes	
8	Font Size	Yes (12)	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map	Yes	

The monogram of the institution is not at the proper place (top left corner).

The title is available on the home page and on the linked pages.

The search option in this site is present on its proper place (top right corner) following the rule which is assistive for the experienced and fresh users to search all the contents of the website which he wants to search by saving precious time.

all the contents of the website which he wants to search by saving precious time.

The breadcrumbs are creating step by step in the site when this site is further visited.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is present on the page of the site which shows all the contents of the site in hierarchy structure, so by clicking on the "Site Map", it will be helpful for the user to see that what contents this site involves.

4. *University of Agriculture, Faisalabad (http://uaf.edu.pk/new/default.aspx)*

S#	Parameters	Yes	No
1	Logo	Yes	Not a Top left , Link
2	Title	yes	Link not available
3	Search		No
4	Breadcrumbs		No
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	Yes	
8	Font Size	Yes (12)	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map		No

The monogram of the institution is present on the home page but is not on its proper place (top left corner) and is not available on the linked pages.

The title of the page is available but there is no link available on the title.

According to the rules, there should be a search option on the top right side of the page on the home

page as well as on the linked pages, but after searching that site, there is no search option on the home page and the linked pages.

There is no creation of the breadcrumbs when the site is further explored.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is not present in the site to assist the user to see the contents of the website in less time.

5. *University of the Punjab, Lahore (http://www.pu.edu.pk/)*

S#	Parameters	Yes	No
1	Logo	Yes	Link
2	Title	yes	Link not available
3	Search	Yes(without no text field)	No
4	Breadcrumbs	Yes	
5	Visited & unvisited Link	Yes(proper color)	No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	Yes	
8	Font Size	Yes	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map	yes	

The logo is present on the home page at top left corner but the link on it is not available.

The title of the page is available but there is no link available on the title.

After visiting this website it has been noticed that there is a search option present on the home page as well as on the linked pages but it is wonderful to see that only the "search" text is present and there is not text field present beside it but when the search text is clicked, the search text field appears.

The breadcrumbs are creating step by step in the site when this site is further explored.

The non visited links appear blue as and when these links are visited, they also change color from blue to another color rather than a purple as according to the rules.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is present on the page of the site which shows all the contents of the site in hierarchy structure, so by clicking on the "Site Map", it will be helpful for the user to see that what contents this site involves.

6. *National University of Sciences and Technology (NUST) (http://www. nust.edu.pk)*

S#	Parameters	Yes	No
1	Logo	Yes	
2	Title	yes	Link not available
3	Search	Yes	
4	Breadcrumbs	Yes	
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	Yes	
8	Font Size	Yes	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map		No

The monogram of the institution is at the proper place on every page.

The title is available on the home page and on the linked pages but a link on it is not available.

The search option in this site is present on its proper place (top right corner) following the rule which is assistive for the experienced and fresh users to search all the contents of the website which he wants to search by saving precious time.

The breadcrumbs are creating step by step in the site when this site is further visited.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is not present in the site to assist the user to see the contents of the website in less time.

7. *Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi (http://www.uaar.edu.pk/)*

S#	Parameters	Yes	No
1	Logo	Yes	
2	Title	yes	
3	Search		no
4	Breadcrumbs	Yes	
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	Yes	
8	Font Size	Yes (12)	10,11
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map		No

Both the logo and title are present, the logo is at its proper place having a link on it but the title has no link on it.

According to the rules, there should be a search option on the top right side of the page on the home page as well as on the linked pages, but after searching that site, there is no search option on the home page and the linked pages.

The breadcrumbs are creating step by step in the site when this site is further visited.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is not present in the site to assist the user to see the contents of the website in less time.

8. *University of Health Sciences, Lahore (http://www.uhs.edu.pk)*

S#	Parameters	Yes	No
1	Logo	Yes	Link not available
2	Title	yes	Link not available
3	Search		No
4	Breadcrumbs		No
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable		No
8	Font Size	Yes (12)	10,11
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map	Yes	

Both the logo and title are available but there is no link available on it.

The search option is also not present and breadcrumbs are also not creating in the website of this institution.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

The back button in this site became disabled when further navigation is encountered which is

problematic for the user because a new window is opened for each navigation and the user cant go back by clicking on the back button which became disabled.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is present on the page of the site which shows all the contents of the site in hierarchy structure, so by clicking on the "Site Map", it will be helpful for the user to see that what contents this site involves.

9. *COMSATS Institute of Information Technology (CIIT), Islamabad http://www.ciit.edu.pk/)*

S#	Parameters	Yes	No
1	Logo	Yes	Link not available
2	Title	Yes	Link not available
3	Search		No
4	Breadcrumbs		No
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable		No
8	Font Size	Yes (13)	10,11
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map		No

In the website of this institution, the logo and title both are present but the link is not available on both of them. The search option and breadcrumbs are also not available in this site.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

The back button in this site became disabled when further navigation is encountered which is problematic for the user because a new window is opened for each navigation and the user cant go back by clicking on the back button which became disabled.

The font size is at least 12pts according to the rules which is assistive for the aged people using that site.

The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is not present in the site to assist the user to see the contents of the website in less time.

10. *Lahore University of Management Sciences, Lahore (http://www.lums.edu.pk/)*

S#	Parameters	Yes	No
1	Logo	Yes	
2	Title	Yes	
3	Search	Yes	
4	Breadcrumbs	Yes	
5	Visited & unvisited Link		No
6	Avoid Scrolling horizontally	yes	
7	Back button enable	yes	
8	Font Size	Yes	
9	Typeface	yes	
10	About us used for org. info	yes	
11	Site Map	yes	

The monogram of the institution is at the proper place on every page

The title is available on the home page and on the linked pages.

The search option in this site is present on its proper place (top right corner) following the rule which is assistive for the experienced and fresh users to search all the contents of the website which he wants to search by saving precious time.

The breadcrumbs are creating step by step in the site when this site is further visited.

When the site was visited for surveying the colors of the visited and non visited links, it was evaluated that the when the links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

The links were navigated for further searching and was back to that link, it was noticed that the color of the visited link was not change to purple which is a big fatigue for the user using the site because he will not be aware of himself that which part of the site he has visited so far.

There is no horizontal scrolling in the website and the user is free of tedious effort to scroll horizontally.

When the site was checked for the back button, it was evaluated that when the different links were visited in the site, we were able to go back (the back button is enable) and the linked contents do not open in the new window, so the user will feel comfortable to use that site and will be enable to visit further links by clicking on the enabled back button.

The font size is at least 12pts according to the rules which is assistive for the aged people using that

site. The typeface in the site used is Verdana and Arial as in the rules.

"About us" is present in the site providing the information of the Institution.

The "Site Map" is present on the page of the site which shows all the contents of the site in hierarchy structure, so by clicking on the "Site Map", it will be helpful for the user to see that what contents this site involves.

II. Conclusion

After detailed study of the websites of different universities/institutions, it has been concluded that most of the institutions/universities do not follow the web usability rules due to which the users (fresh & experienced) face different problems exploring these sites and also a time consuming process. When the user visits a site which has no usability rules became bored in the first time of the exploring and never visits this site again. Different universities/institutions must follow the usability rules to facilitate the user in encountering different tasks which leads to time consuming free exploring tasks. Different parameters were analyzed in light of usability in the websites of different universities in Pakistan. It was evaluated that these universities websites have the errors in the parameters not following the rules of usability. The usability of websites of different universities/institutions of Pakistan can be improved applying the one rule for every factor so that the user can encounter every task easily with no tedious effort and confusion. These rules of usability should be announced by the government and the universities should be limited in these rules to facilitate the fresh and experienced users.

References Références Referencias

1. Jacob Nielsen's Alertbox: January 4, 2012. http://www.nngroup.com/articles/usability-101-introduction-to-usability/
2. http://guidelines.usability.gov/guidelines/154
3. http://www.nngroup.com/articles/ten-good-deeds-in-web-design/
4. http://guidelines.usability.gov/guidelines/189
5. http://guidelines.usability.gov/guidelines/78
6. http://guidelines.usability.gov/guidelines/98
7. http://guidelines.usability.gov/guidelines/79
8. www.usability.gov/guidelines/guidelines_book.pdf
9. http://www.nngroup.com/articles/let-users-control-font-size/
10. http://www.nngroup.com/reports/senior-citizens-on-the-web/
11. http://webstandards.hhs.gov/standards/10
12. http://www.nngroup.com/reports/about-us-presenting-company-information/
13. http://guidelines.usability.gov/guidelines/76

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme

By Gorti VNKV Subba Rao & Dr. Garimella Uma
Sree Dattha Institutions, India

Abstract - In MANETs the nodes are capable of roaming independently. The node with inadequate physical protection can be easily captured, compromised and hijacked. Due to this huge dependency's on the nodes, there are more security problems. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer. In this paper we look at the current scheme to transmit the data in MANETs. We then propose a new scheme for secure transmission of message in MANETs as Alternative scheme for DF's new Ph and DF's additive and multiplicative PH. Here we also provide the computational cost of the homomorphic encryption schemes. We also provide the implementation issues of our new scheme in MANETs. For the entire message to be recoverd by the attacker, the attacker needs to compromise atleast g nodes, one node from each group g and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network.

GJCST-E Classification : *E.3*

AN EFFICIENT SECURE MESSAGE TRANSMISSION IN MOBILE AD HOC NETWORKS USING ENHANCED HOMOMORPHIC ENCRYPTION SCHEME

Strictly as per the compliance and regulations of:

An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme

Gorti VNKV Subba Rao [α] & Dr. Garimella Uma [σ]

Abstract - In MANETs the nodes are capable of roaming independently. The node with inadequate physical protection can be easily captured, compromised and hijacked. Due to this huge dependency's on the nodes, there are more security problems. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer. In this paper we look at the current scheme to transmit the data in MANETs. We then propose a new scheme for secure transmission of message in MANETs as Alternative scheme for DF's new Ph and DF's additive and multiplicative PH. Here we also provide the computational cost of the homomorphic encryption schemes. We also provide the implementation issues of our new scheme in MANETs. For the entire message to be recoverd by the attacker, the attacker needs to compromise atleast *g* nodes, one node from each group *g* and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network.

I. Gorti's-Enhanced Homomorphic Cryptosystem (EHC)

A new Enhanced homomorphic Cryptosystem (EHC) for homomorphic Encryption / Decryption with IND-CCA secure. Homomorphic encryption schemes allow operations to be performed on the encrypted data as if the operations are performed on the plaintext. Homomorphic encryption has numerous applications in real time. The computer will perform the computation on the encrypted data, hence without knowing anything of its real value. Finally, it will send back the result, and that will be decrypted. For coherence, the decrypted result has to be equal to the intended computed value if performed on the original data. For this reason, the encryption scheme has to present a particular structure [23].By keeping the all the industry demands we proposed new scheme exhibit better performance than existing schemes mainly in processing speed, memory and power consumption. Our scheme is a non deterministic and exhibits addition, multiplication, mixed addition and mixed multiplication operations. Our Construction. A large prime number 'p', another prime number 'q' such that q < p are taken and a random number 'r' has taken to make the scheme non deterministic. Consider the set of clear text data *Zp* and the set of clear text operations *{+, -,*, / and mixed}* consisting respectively, of the addition, subtraction, multiplication and mixed multiplication modulo m, with *m= pq.* Let the cipher text data set be *Zc*. Define the encryption key k = (p, *q,m,r)* and Ek(X)=)(mod m). *Decryption will be done with the secret key* k = (p), X=Dk (Y) = C mod p. But can be broken if *p* can be discovered but which is a very tough to solve. A computer can factor that number fairly quickly, but (although there are some tricks) it basically does it by trying most of the possible combinations. One can find two huge prime numbers, p and q that have 200 or may be 400 digits each. Q will be kept secret (It is secret key), and by multiplying them together to make a number m = pq. That number m is also a secret key to encrypt the data. It is relatively easy to get m by multiplying p and q. But if anybody know m, it is basically impossible to find p and q . To get them, you need to factor m, which seems to be an incredibly difficult problem finding the ' r ' also difficult as this value will be generated randomly. it is generally regarded that m should be at least 1024, if not 2048.

a) Operations Encryption/Decryption of EHC Scheme

Secretkeygen()
Chose large prime number ' p ' and another prime number ' q ' Calculate m = p * q Generate a random number ' r '. r,q and m Kept secret. Secret values r,q and
m Shared key : p
Encryption Encrypt(X,m,p,q,r) Assume $X \in Z_p$ Compute $Y = (X + r*p^q) \pmod{m}$ Output $Y \in Z_c$
Decryption Decrypt(Y,p) input $Y \in Z_c$ compute X = Y mod p output $X \in Z_p$

Algorithm of EHC

Author α : Vice Principal,Sree Dattha Institutions, Hyderabad.
E-mail : gvnkvsubbarao@yahoo.com
Author σ : Director & Professor, Teachers Academy, Hyderabad.

In order to see that the scheme above deciphers correctly it is necessary to prove that decryption really outputs the original message M.

Proof : Encrypt the message X

$$E(X) =)(\text{mod } m)$$

Cipher text Y will be (X+rp)

Decrypt Y = X = Y mod p

= (X+rp) mod p

= rp mod p + X mod p

= X Plaintext

b) Security of the Encryption Scheme

We can support strongly our scheme is more secure when compare to existing schemes as follows :

1. Our scheme is very strong as it uses the secret keys q, m and r and sharing key p for encryption. So it is very difficult to find the secret keys.
2. Our scheme only shares the shared key p only between the sender and receiver so it is very difficult to find the q and r.
3. Random number 'r' will be generated randomly so that every time the same plaintext mapped to different cipher text so that it is very tough to track the plain text even with strong observation for opponent.
4. Opponent cannot get the secret value and random number.
5. Our scheme supports Addition, Multiplication, Mixed addition and Mixed multiplication.
6. As we are taking large prime number p the decryption circle will be more so that second multiplication also possible.
7. Is IND-CCA secured scheme which will be proved in the next section.
8. It is very faster than the existing schemes and consumes less power and memory.

c) Non deterministic feature which enhances the security

The random number 'r' gives the feature non deterministic means the plaintext will be converted into different cipher text with the change in the value r. We can better understand using the following example.

Let p=11 q=7 r=2 x1=5 x2=3 then m=77 cipher text Y1= 27 cipher text Y2= 25.

Now by changing the random number the same plain text will be mapped to another cipher texts Let p=11 q=7 r=4 x1=5 x2=3 then m=77 cipher text Y1= 49 cipher text Y2= 47.

II. Introduction to MANETs

Mobile Ad-hoc network (MANETs) is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. By definition, MANETs differentiate themselves from existing networks by the fact that they rely on no fixed infrastructure [Zhou and Haas 1999]: the network has no base stations, access points, remote servers, etc. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1.1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

Technically and architecture wise if we see the MANETs environment consists of mobile nodes that communicate directly with each other in a peer to peer way. Mobile nodes that join together in on movement and they create a network on their own and each these node performs the basic operations like routing and packet forwarding without the help of an established infrastructure. All the available nodes can join together in the network and carry out network operation. Due to this huge dependency's on the each other nodes it is obvious to have more security problems. Other angle if we observe in MANETs, the nodes are capable of roaming independently so that the node with inadequate physical protection can be easily captured, may compromise and hijacked. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer [12, 13].

Security is an important area for MANETS, especially for those comes under security-sensitive applications. To provide security in MANETs, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.[81] Mobile ad hoc networks are self configurable and autonomous systems, comprising of nodes, which are able to move and organize themselves arbitrarily without any infrastructure [1]. Without the support of infrastructure, it is very difficult to distinguish the insider and outsider nodes of the mobile ad hoc networks. Since the mobile adhoc network environment is defined in a unique way, by features such as frequently changing network topology, vulnerable wireless links, storage limitations, and constraints in computational and transmission aspects [2]. Due to the above-mentioned properties of MANETs, the inclusion and implementation of security infrastructure has been a real challenge.

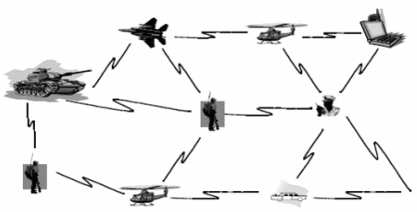


Figure 1.1 : Overview of Mobile Ad-hoc Network

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Wireless ad-hoc network have many advantages:

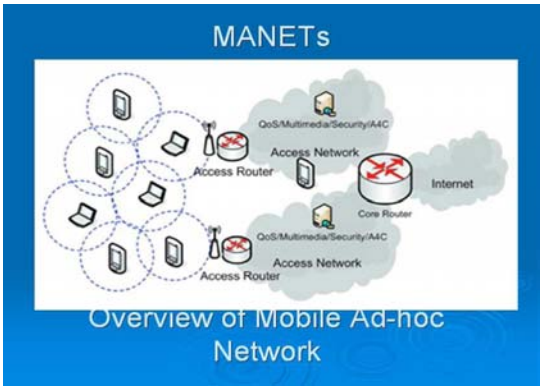
– *Low Cost of Deployment :* Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
– *Fast Deployment :* Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
– *Dynamic Configuration :* Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future in MANET, provision of secure communication protocol should satisfy the following security requirements [7, 8, 9].

1. *Mutual Authentication :* Ensures the authenticity of communicating nodes mutually.
2. *Confidentiality :* Ensures the secrecy of the message content is known only between the authenticated communicating nodes (or users).
3. *Data Integrity :* Ensures the receiver, that the received message is intact.
4. *Non–Repudiation :* Ensures the origin of the message cannot deny having sent the message.
5. *Non–Impersonation :* Ensures unauthorized users cannot pretend to be an authorized one to do malfunction. Proposed novel protocol achieves the above security requirements and also requires less computational power due to the deployment of elliptic curve cryptography and minimum transmission overhead due to less number of handshaking messages.

First we will discuss in detail the existing security solutions available for MANETs. Then we propose a new scheme for secure transmission of message in MANETs as an alternative for threshold cryptography (TC).

III. Literature Survey



Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that uses temporary network from existing network infrastructure or central point. Each node participating in the network acts as host/a router and must forward to packets for other nodes. MANETs are completely different from other network because of their characteristics such as: self organizing capability, node mobility, provides large number of degree of freedom and dynamic topology. As mobile ad hoc networks edge closer toward wide-spread deployment, security issues have became a central concern and are increasingly important.

In fact, ad hoc networks cannot be used in practice if they are not secure, for example, in applications like emergency rescue and battlefield communication; if no security mechanism is used, an adversary can easily thwart the network establishment. Due to their inefficiency, asymmetric/public key cryptosystems, for example RSA, are unsuitable for ad hoc networks where there are constraints on computation and energy [10]. In fact, symmetric key systems, like DES, AES and keyed hash functions, are still the major tools for communication privacy and data authenticity in most networks. To provide secure communication for any group of nodes using symmetric key cryptography, these nodes need to share a common secret key1 By definition [30], an ad hoc network is peer-to-peer and does not rely on any fixed infrastructure.

A *mobile ad hoc network* (MANET) [1] is a collection of wireless mobile nodes that form a temporary network on the fly that operates without the support of any fixed network infrastructure. MANETs are created dynamically and they provide special challenges beyond those in standard data networks [2]. Some examples of the possible uses of ad hoc networking [3],[4] include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or

earthquake. In such networks, each mobile node operates not only as a host but also as a router and cooperates dynamically to establish routing among them to discover "multihop" paths through the network to any other node.

There are various issues related to ad hoc networks [5], [6]. Several protocols have been proposed for routing in such an environment.

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network.

Mobile Ad Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread application in military and civilian communications. Such a network is highly dependent on the cooperation of all of its members to perform networking functions.

IV. Advantages of Manets

The following are some of the advantages of mobile ad hoc networks.

i. They provide access to information and service regardless of geographic position. This is applicable in military or police exercises, disaster relief operations, mine site operations, and urgent business meetings, where instant communication is needed.
ii. These networks can be setup at any place and time. They can be setup without wires or base stations and the nodes are free to move randomly and organize themselves arbitrarily; thus the networks wireless topology may change rapidly and unpredictably. Mobile devices in the network can freely leave or join the network at will.
iii. The networks work without any preexisting infrastructure. This makes MANETs cost effective for areas where there are no standard communication infrastructures. Owners of MANET equipped devices can communicate with each other, share data and streaming video.
iv. Low Power Consumption is another strong point for MANETs. Most devices used are battery powered; hence they are portable, making mobility easy and devices affordable. Examples are Bluetooth enables phones, laptops, palm tops, etc.

V. Challenges of Mobile Ad-Hoc Networks

Some challenges mobile ad hoc networks face towards efficient delivery of service includes:

a) Routing is a Most

Required function in any network. In ad hoc networks, routing poses two specific challenges. Firstly, routing in traditional networks (examples: the Internet and cellular networks) aims to quickly propagate changes in topology or reach ability, hence creating stable networks, while in mobile ad hoc networks, the topology is constantly changing and is deemed unstable. Secondly, traditional routing solutions rely on some form of distributed routing databases, maintained by the operators in either the networks nodes or specialized management nodes. In mobile ad hoc networks, nodes cannot be assumed to have persistent data storage, and they cannot always be trusted [Hubaux, et al 2001].

b) Mobility Management

A network must manage the mobility of its terminals, and therefore be able to locate any of them. In particular, if a terminal wants to communicate with another, it will make use of the address of the latter; the network will have to locate it in some way. The simple solution of broadcasting a paging message to the whole network does not scale. For example, in cellular networks, the location of the mobile stations is stored in centralized servers. The self-organization of ad hoc networks precludes the existence of such servers, leading to mediate loss/trace of any node once outside the range of the immediate network.

c) IP (Internet Protocol) Addresses

For small mobile ad hoc networks, addresses are allocated in the traditional way, with an IP prefix identifying the mobile ad hoc network. For large-scale networks, the topology based address allocation currently used in the Internet may not be optimal. In contrast, a node address should be interpreted as a stable node identifier, which carries no specific topological information.

d) Transport Layer

Of ad hoc networks also requires attention. Transmission and Control Protocol (TCP) performance in ad hoc networks may be severely degraded, as TCP interprets losses as a signal of congestion and this adversely reduces its sending rate, whereas wireless links may temporarily exhibit high loss rates due to transmission errors not related to congestion.

e) Radio Interface

This can be engineered in different ways, based on the requirements of a specific system. Issues to be taken into account include:

i. The decrease in signal strength as the square of the distance.
ii. Some of the traditional multi-access protocols used for wire line LANs cannot be used; example: collision detection is not appropriate because a node is usually unable to listen while it is transmitting.
iii. Two terminals may unknowingly interfere at a third one.

f) Security

This is of critical importance for most networks, and mobile ad hoc networks are no exception. Several security features can be required, such as availability of service despite denial-of-service attacks, confidentiality, integrity, authentication, and non-repudiation. Guaranteeing these features is a major challenge.

g) Power Management

Is almost always a difficult issue in wireless networks. In the case of ad hoc networks, there are essentially two concerns:

i. Power has to be fine-tuned in order to maximize the throughput of the network: the higher the power, the larger the transmission ranges of the node, but also the higher the interference from other signals. Trade-off is obtained when there is on average exactly one packet in transit over each hop.
ii. Since the nodes are usually battery operated, it is important to minimize their consumption. A typical solution consists in turning the devices to a sleep or idle mode whenever they

VI. Existing Security Solutions Available in the Area MANETs

1. Secure routing protocol
   a) Secure Routing Protocol (SRP) [9, 10].
   b) Secure link state protocol (SLSP) [11].
2. Secure data forwarding
   a) Secure Message Transmission (SMT) [12,13]
   b) Threshold Cryptography (TC) [14].

In detail we can see below.

a) Secure routing protocol suggested for MANETs (SRP)

There are various secure routing protocols suggested for routing packets in MANETs. One such routing protocol is Secure Routing Protocol (SRP) [9, 10]. In SRP, only the end nodes have to be securely associated, with no need for cryptographic operations at the intermediate nodes. SRP provides one or more route replies, whose correctness is verified by the route "geometry" itself, while compromised and invalid routing information is discarded. Another routing protocol is secure link state protocol (SLSP) [11] for MANETs. It uses the secure neighbor discovery and the use of neighbor lookup protocol (NLP) strengthens SLSP against attacks that attempt to exhaust network and node resources. Furthermore, SLSP can operate with minimal or no interactions with a key management entity, while the credentials of only a subset of network nodes are necessary for each node to validate the connectivity information provided by its peers.

b) Secure Data Forwarding Suggested for MANETs

We will see two major secure message transmission schemes such as Secure Message Transmission and Threshold Cryptography.

c) Secure Message Transmission

Secure routing is the pre-requisite for implementing secure data forwarding. The main concept here is forwarding data securily in MANETs in the presence of malicious /untrusted nodes after the discovering the route between the source and target. There are various schemes with various factors proposed for secure data forwarding such as data forwarding based on neighbor's rating, implementing currency system in network for packet exchange, and redundantly dividing and routing message over multiple network routes. For example, Secure Message Transmission (SMT) is a secure data forwarding scheme in which first the active paths are discovered between two nodes using secure routing protocol. Based on B active paths, the message is divided into B different parts such that any A parts can be used to recover this message. These B partial messages are then routed on the identified paths. The destination can recover a message when A or more partial messages are received. Thus, this scheme ensures that the message reaches the destination even if a few packets are dropped in transit. Both the above security solutions are essential to ensure that the MANETs survive even in the presence of malicious or untrusted nodes. Thus, by implementing the above solutions the nodes can communicate securely without relying on all nodes on only one route. The concept of dividing the message using SMT protocol is extended further in the Threshold Cryptography can be implemented to redundantly fragment the message into B parts such that using any T parts the message can be recovered [12, 13, 14]. Now we will see in detail about the this.

d) Threshold Cryptography

The main goal of threshold cryptography (TC) is to split a cryptographic operation among multiple users so that some predetermined number of users can perform the desired (cryptographic) operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and/or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key.

The power to sign should then be shared, to avoid abuse and to guarantee reliability. Main aim of TC is to make this possible. Both the schemes ECC and RSA are homomorphic. Therefore, threshold cryptography is applicable and cryptographic operations can be split among multiple users such that any subset comprising of *t* users can perform the desired operation, where *t* is a predefined number. In a *t* out of *n* scheme, any set of *t* users can perform the desired operation, while any set of (t-1) users or less cannot. A cryptographic scheme based on threshold cryptography is secure against an attacker as long as the attacker compromises no more than (t-1) nodes.

Threshold cryptography (TC) [13, 14, 15] involves sharing of a key by multiple individuals called shareholders engaged in encryption/decryption. The aim of this is to have distributed architecture in a hostile environment. Other than sharing keys or working in distributed manner, TC can be implemented to redundantly split the message into B parts such that with T or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over B multiple paths. Threshold schemes generally involve key generation, encryption, share generation, share verification, and share combining algorithms. The basic requirement of any TC scheme is Share generation, for data confidentiality and integrity. Threshold models can be broadly divided into two major First one is single secret sharing threshold e.g. Shamir's *t-out-of-n* scheme based on Lagrange's interpolation and later one is threshold sharing functions e.g. geometric based threshold. These schemes are being used to implement threshold variants of RSA, ElGamal,ECC and Privacy Homomorphism[13, 14]. RSA-TC and ECC-TC has been discussed in the papers [13, 14, 15]. It has been shown that RSA-TC using key sharing is unsuitable in resource constrained MANETs due to high storage, computation, and bandwidth requirements [13].

ECC-TC has been shown to be more efficient for resource constrained MANETs [14]. The authours in paper [14] has used variation of ECC implemented algorithms such as Diffie-Hellman (DH), Menezes Vanstone (MV) and L Ertaul in MANETs. They have performed various comparison tests in different scenarios between these different ECCs'. ECC-DH split before encryption has been proved to be better for resource constraint sender as the encryption timings are lowest. ECC-MV split before encryption has been proved to be best for decryption at the resource constraint receiver as the decryption time is lowest. The encryption and decryption time of ECC- MV and ECCDH has been shown to vary significantly for encryption before split and encryption after split. The encryption and decryption time of ECC-Ertaul has been proved to be more moderate for varying key sizes, T and B for both encryption before split and encryption after split. As a result ECC-Ertaul has been suggested as a best variation of ECC for MANETs in his experiment results [14]. We will show by our observations in our experiments how our Enhanced homomorphic encryption scheme can be used as an alternative for TC for performing the transmission the message securely in MANETs in the next section.

e) MANETs – New Protocol by Implementing EHES

In ECC based TC there is an overhead of message splitting using Lagrange Interpolation scheme. In our new scheme keeping the concept of threshold cryptography in mind, the message can be split and encrypt by the our Enhanced homomorphic encryption scheme removing the overhead discussed above by Lagrange Interpolation all together. In our scheme we increase the success rate as compared to RSA based TC. In our study we used the Elgamal, MMH along with our Enhanced Homomorphic encryption scheme to encrypt the message. We also tested their encryption times and execution times. Here we will discuss about our new protocol to transmit the encrypted message securely by using our Enhanced homomorphic encryption schemes. We show that even if a node is compromised, the node will not be able to determine the sensitive information. Even if certain number of nodes are compromised and not send the message, the destination can recover the message.

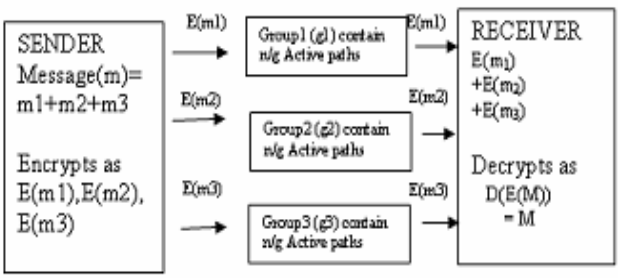


Figure 1 : New Protocol in MANETs

In our protocol we are only interested in secured message transmission securely on the already established path not in path establishment from the sender to the receiver. We assume that set of disjoint paths and the key (using any of the key distribution schemes.) have already been established from the sender to receiver by MANETs routing protocols [9, 10] between the sender and receiver.

To transmit the message securely, the idea is to group the set of *n* disjoint paths from sender to receiver into *g* groups, each group having at least *n/g* active disjoint paths. The message to be transmitted is split into number of messages equal to *g* and encrypted using homomorphic encryption schemes [2,3,4,5]. The encrypted split message is sent to each of the *g* groups so that the each group having only one encrypted split message. Each node (router) in the group also will have

the same split message and the entire message cannot get even if node compromised. As Homomorphic encryption schemes are used to encrypt the split message, by performing addition operation on the encrypted split messages the receiver can recover the entire encrypted message and decryption the entire recovered message. This scheme is illustrated in the *Figure 5.1.*

As we know, the nodes are always on the move in MAMETs. There will be scenarios where the intermediate node is out of range or may have been killed or out of the MANET all together. In such cases how would the receiver get all the split messages sent by the sender? It is the serious question. To ensure that the receiver gets all the split messages, the sender sends the same split messages to more than one disjoint paths. Let us assume that there are *n* disjoint paths and the disjoint paths getting the same split message belongs to one group. Let us assume that there are *g* groups of disjoint path, with each group having at least *n/g* disjoint paths. The sender splits a message into *g* splits, and sends each split to each group. The receiver recovers the entire message even if at most *(n/g)-1* disjoint paths are not active. A malicious node cannot recover the entire message as it gets only partial encrypted message. To ensure security the sender does not send more than one split message to the same group of nodes.

f) Secure data forwarding protocol with EHES implementation results

We simulated the MANETs environment using the programming language C in the Linix environment. It is done on a system having the Intel® Core™ 2 Duo CPU T5750@2GHz CPU and 3 GB system memory running the Linux kernel –2.6.25-14.fc9.i686 Fedora release -9.

The assumptions during implementation are that there is a sender, receiver and multiple forwarding nodes between them and set of active disjoint paths have already been established from the sender to receiver by the routing protocols. We also assume that the key for homomorphic encryption scheme has already been established between the sender and receiver by using any of the key distribution schemes. The Homomorphic encryption scheme used to encrypt the message at the sender are Enhanced Homomorphic encryption scheme, Mixed multiplicative homomorphism and Elgamal. Using our simulation system, We have tested all the schemes processing timing encryption timings. Here we also tested the following scenarios

1. By varying key sizes 512, 1024 and 2048 bits by keeping the message size fixed.
2. By varying message sizes 500, 1000, 2000 bits as on stream and 100, 250, 500 bits as in another streams with fixed key size (512,1024 and 2048 bits).
3. By varying d (splitting times) size 2,4,6,8,10 to find the best d value in the Network as the d is based on number of groups.
4. Here we have considered the following two
   – First one, encryption done after the splitting the message.
   – Second one, Encryption done first and then split the message.

In our simulation the active disjoint paths getting the same message are grouped as one group. Based on *n* active paths the groups *g* are determined. The sender splits the message and encrypts each split message with the one of the homomorphic encryption schemes. In our network, *n* and *g* are fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24})*. The proposed network rate of success is computed as (*No. of recovered messages by the receiver/No. of sender sent message s*) * *100 … (5.1)* The rate of success of the network with *n* and *g* fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24})* is determined by randomly killing the nodes. The nodes are killed randomly by using Exponential distribution provided by the function in GSL library [41].

In our implementation, the sender first splits the message into *g* partial messages where each partial message is sent to one of the *g* groups of the MANETs. Each of the partial messages are associated with a unique message split id. All the message split id's of the partial messages forming the entire message is summed up to set up the message split id sum. The message id, message split id, message spit id sum and encrypted partial text is placed in the buffer so that the receiver can recover the entire message from the partial encrypted message. To recover the entire message sent by the sender, the receiver follows two steps. In the first step the receiver adds up all the partial encrypted message whose message id's are same and message split id's sums up to message split id sum. In the second step the receiver decrypts the sum of all partial encrypted messages to recover the entire message. As the same encrypted partial message is sent to all the active paths in the group the receiver is likely to get the same redundant message. The redundant messages will be discarded by the receiver if they have the same message id and message split id. In the next section we look at the encrypted message buffer structure.

g) The encrypted message buffer structure

The size of the encrypted message buffer structure sent form sender to receiver varies from one homomorphic encryption to another.

h) Elgamal

In elgamal the size of the cipher text increases with the increase in the encryption split *"d"*. So the size of the buffer increases with the increase of the parameter *d* used in encryption.

i) Mixed Multiplicative Homomorphism (MMH)

Here also the size of the ciphertext increases with the increase in the encryption split *"d"*. So the size of the buffer increases with the increase of the parameter *d* used in encryption.

j) Enhanced Homomorphic Encryption Scheme (EHES)

In all the above mentioned schemes the *message id* field identifies different messages encrypted at the sender. The messages split at the sender is uniquely identified by *message split id*. The sum of all the *message split id* is included in *message split id sum*. The rest of the buffer is used to contain the size of the ciphertext and the ciphertext itself. The size of the ciphertext is essential in reading the ciphertext from the buffer. The receiver recovers the entire message by adding up all the cipher values with the same message id and whose *message split id's* adds up to *message split id sum.*

k) Experimental Investigations

We will see the performance results from our simulation.

In MANETs as we know that the nodes have low computational power, Less memory. In such cases we need to find best encryption scheme, which can compute fastly and occupies less memory. In our implementation we do various tests to find a relatively best encryption schemes among our scheme, Elgamal, MMH.

In our simulation we tested and determined the encryption timings of all above mentioned encryption schemes by varying the key size (512, 1024, 2048 bits) and keeping the message size fixed (512 bits). In another test we determined the execution timings of all these same encryption schemes by keeping the key size fixed (512 bits, 1024 bits, 2048 bits) and varying message size. The timings are determined over 200 runs.

Figure 1 represents the execution timings of *Table 1* in a chart. From *Figure 1*, by observation we found clearly that our Scheme is much faster than other encryption schemes. We also observed that the encryption timings of Scheme MMH and Elgamal increases with the increase in encryption keys but in case of our Scheme the encryption timing remains almost the same with the

Message size in bits	Elgamal	MMH	EHES
250	89	21	9
500	105	21	11
1000	142	22	8

Table 1 : Encryption process time of Schemes μSec with key size 512 bit increase in the encryption key size

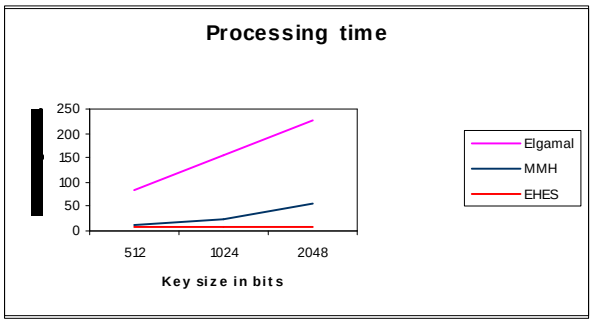


Figure 1 : Processing time of Schemes in micro seconds with varying key sizes and fixed message size 512 bits

Table 1 represents the execution timing of above mentioned schemes in micro seconds by increasing the message size to 100, 250 and 500 bits and by keeping the key size fixed (512 bits). *Figure 1* graph represents the execution timings of *Table 1.* From *Figure 2*, it is very clear that our Scheme is much faster than other two Schemes. We also found that the encryption timing of other Schemes increases with the increase in message size we also observed that the Message size encryption timings of our Scheme remains almost the same with the increase in the message size.

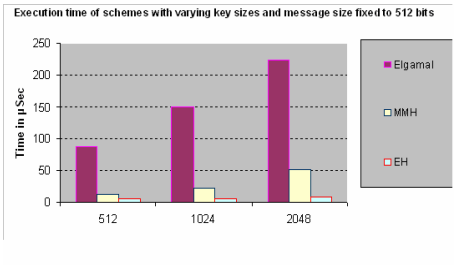


Figure 2 : Encryption process time of Schemes in μSec with key size 512 bit

Table 3 represents the execution timings of the same encryption schemes in micro seconds by increasing the message size (250, 500 and 1000 bits) and by keeping the key size fixed (1024 bits). *Figure 3* graph represents the execution timings of *Table 37.*. From *Figure 5.4*, we can say that our Scheme is much faster than other schemes. We also observed that the encryption timings of Elgamal increases with the increase in message size and the encryption timings of our Scheme and MMH remains almost the same with the increase in the message size.

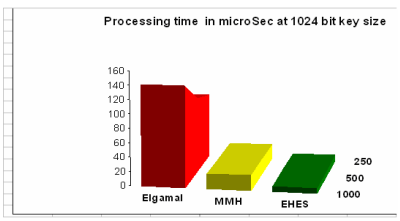


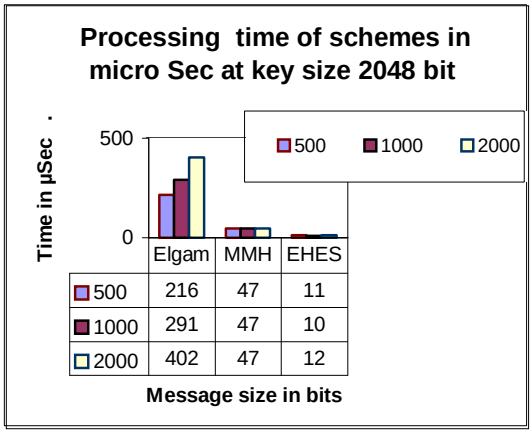
Figure 3 : Processing time of schemes in μSec at 1024 bit key size

Table 3 : Processing time of schemes in μSec at 1024 bit key size

MESSAGE SIZE IN BITS	Elgamal	MMH	Our Scheme EHES
100	72	11	7
250	76	11	7
500	87	11	7

We have also computed the execution timings of Schemes in micro seconds by increasing the message size (500, 1000 and 2000 bits) and by keeping the key size fixed (2048 bits). graph 4 shows the execution timings computed, it is observed that our Scheme is much faster than other schemes as shown in chart and that the encryption timings of Elgamal Schemes increases with the increase in message size and the encryption timings of our Scheme and MMH remains almost the same with the increase in the message size.

Figure 4 : Processing time of schemes in μSec at key size 2048 bit



From the graphs and corresponding *Tables* it is observed that our Scheme is much faster than other schemes. We also observed from graph (*Figure 2)* that the encryption timings of other Schemes increases with the increase in encryption keys but the encryption timing of our Scheme remains almost the same with the increase in the encryption key size. From graphs and corresponding *Tables* we also can say that the encryption timings of Elgamal Scheme increases with the increase in message size. However the encryption timings of MMH and our Schemes remains almost the same with the increase in the message size.

I) Experimental Results of our New Protocol with our new scheme

In MANETs we know that the nodes are always on the move and there may be scenarios where the active path may no longer be active with this result, the receiver may not receive all the packets sent by the sender. *Figure 5 graph* depicts the rate of success of the networks with *n* active paths and *g* groups fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24}),* by randomly killing the nodes. The nodes in the networks are killed randomly by using Exponential distribution provided by the function in GSL library [41].

The networks with *n* and *g* fixed to *(12,{2,6,12})* defines 3 sets of networks with the I network having *12* active paths, *2* groups and 6 active paths in each group, II network with *12* active paths, 6 groups and *2* active paths in each group and III network with *12* active paths, *12* groups and *1* active path in each group. The networks with *n* and *g* fixed to *(16,{2,8,16})* defines 3 sets of networks with I network having *16* active paths, *2* groups and 8 active paths in one group and *8* active paths in another group, II network with *16* active paths, 8 groups and 2 active paths in one group and *2* active paths in remaining groups and III network with 16 active paths, *16* groups and *1* active path in each group. The networks with *n* and *g* fixed to *(24,{2,12,24})* defines 3 sets of networks with I network having *24* active paths, *2* groups and *12* active paths in each group, II network with *24* active paths, *12* groups and *2* active paths in each group and III network with *12* active paths, *24* groups and *1* active path in each group. From graph shown in the *Figure 5.7* it is clear that the rate of success increases by reducing the number of groups in the network. This is because by reducing the number of groups in the network we would increase the number of active paths in each group. Just one partial message from each group is enough to recover the entire message. From *Figure 5.7* we see that the rate of success is 100% with *g=2* and *n=12,16,24.* This is because by increasing the number of paths in each group, the probability of one path in each group remaining active is high and with it the probability of recovery of the message at the receiver is also high. The rate of success gradually decreases with the gradual increase in the number of groups in the network. With *g=n* we see that rate of success is lesser than 50%. Therefore to get the rate of success as 100% in the network it is better to reduce the number of groups, thus increasing the number of active paths in each group.

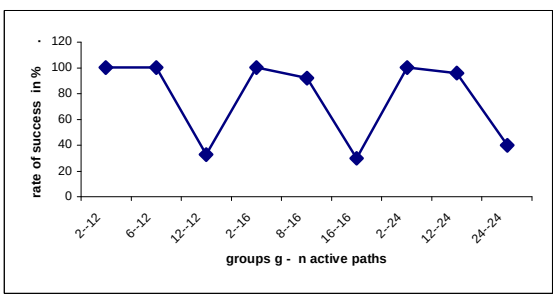


Figure 5 : Rate of success of the I,II & III Network

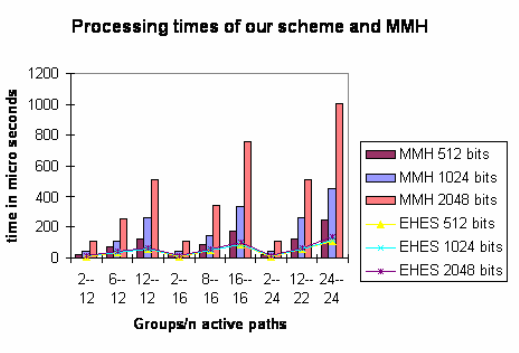


Figure 6 : Processing timing (in micro seconds) of our Scheme and MMH in micro Seconds varying key sizes 512, 1024 & 2048

Table 4 : Processing timing of our Scheme and MMH in micro Seconds varying key sizes 512, 1024 & 2048

	MMH Scheme with bey size in bits			Our Scheme with bey size in bits		
Group Out of n Active Path	512	1024	2048	512	1004	2048
2-12	25		112	10	11	14
6-12	70		254	34	35	40
12-12	124		515	55	60	68
2-16	25		112	10	11	14
8-16	85		339	50	50	55
16-16	177		760	85	90	103
2-24	25		112	10	11	14
12-22	124		515	55	60	68
24-24	243		1008	112	115	140

In our proposed protocol in MANETs the sender splits the message with respect to the value *g*. The sender using the homomorphic encryption scheme then encrypts all the split messages. As the number of splits at the sender is equal to the value *g* the total encryption timing of all the split messages increase with the value *g*. *Figure 5.7 & 5.8* and the corresponding *Tables* represent the total encryption timings of all the split messages. From the *Figures* it is observed that the total encryption timing increases with the value *g*. Also from *Figures* we found that our Scheme is the much fastest encryption scheme, followed by other Schemes.

VII. Discussion of Results

By using our proposed new scheme for secured transmission of message in the area MANETs as an alternative to TC, we eliminate the overhead of the schemes associated with Lagrange Interpolation Scheme. As MANETs are grouped mode even if one compromised the entire message would not be revealed. For this the attacker needs to compromise atleast *g* nodes to get full message for that he has to get one node from each group *g* and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network. From our implementation results it is clear that our scheme is the fastest homomorphic encryption scheme in comparison with other schemes.

References Références Referencias

1. J. Domingo-Ferrer. "A Provably Secure Additive and Multiplicative Privacy Homomorphism". Information Security Conference, LNCS 2433, pp 471–483, January 2002.
2. J. Domingo-Ferrer, "A new Privacy Homomorphism and Applications", Elsevier North-Holland, Inc, 1996.
3. J. Domingo-Ferrer and J. Herrera- Joancomarti. "A privacy homomorphism allowing field operations on encrypted data". I Jornades de Matematica Discreta I Algorismica, Universitat Politecnica de Catalunya, March 1998.
4. Hyungjick Lee, Jim Alves- Foss, Scott Harrison, "The use of Encrypted Functions for Mobile Agent Security", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.
5. J. Girao, D. Westhoff and M. Schneider. Concealed data aggregation in wireless sensor networks. ACM WiSe04 – poster, in conjunction with ACM MOBICOM 2004, October 2004.
6. J. Girao, D. Westhoff and M. Schneider. CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. 40th International conference on communications, IEEE ICC 2005, May 2005.
7. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans". On Information Theory, 1986.
8. William Stallings "Network Security Essentials", Second Edition, Prentice Hall 2006, pp.3.
9. P. Papadimitratos, Z. J. Haas "Secure Data Transmission in Mobile Ad Hoc Networks," ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.
10. Mithun Acharya, Joao Girao and Dirk Westhoff. "Secure comparison of encrypted data in wireless sensor networks". In 3rd Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Trentino, Italy, April 2005. WiOpt2005.
11. P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan. 27- 31, 2002.
12. P. Papadimitratos, Z. J. Haas, and P. Samar, "The Secure Routing Protocol (SRP) for Ad Hoc Networks," Internet Draft, draft papadimitratos-secure-routingprotocol-00.txt, Dec. 2002.

13. P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proceedings of the IEEE CS Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, Jan. 2003.
14. L. Ertaul, N. Chavan, "Security of Ad Hoc Networks and Threshold Cryptography", 2005 International Conference on Wireless Networks, Communications and Mobile Computing, Wirelesscom 2005, MobiWac 2005, June 2005, Maui, Hawaii.
15. L. Ertaul, N. Chavan, "Elliptic Curve Cryptography based Threshold Cryptography (ECCTC) Implementation for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, pp 48-61 April.
16. L. Ertaul, W. Lu, "ECC based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in Mobile Ad Hoc Networks (MANET) I", Proc. Of Networking 2005 International Conference, May 2005, University of Waterloo, Ontario, CA.
17. Makoto Yokoo, Koutarou Suzuki, "Secure Multi-agent Dynamic Programming based on Homomorphic Encryption and its Application to Combinatorial Auctions", Proceedings of the First International joint Conference on Autonomous Agents and Multiagent systems(AAMAS), 2002.
18. N. Koblitz, "ECC", Math. Of Computation, v. 48, 1987, pp. 203-209.
19. A. J. Menezes, D. B. Johnson, "ECDSA: An Enhanced DSA", Invited Talks – 7th Usenix Sec., Symp., Jan., 1998, pp. 33-43.
20. Certicom Corp., "Certicom ECC Tutorials".
21. Certicom Corp., "Remarks on the Security of the ECC systems", ECC White Papers, uly 2000.
22. K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, vol. 11, no.1, pp. 62-67, February 2004.
23. L. Ertaul, W. Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)", Proc. Of the Networking 2005 International Conf., May 2005, University of Waterloo, Ontario, CA.
24. L. Ertaul, "Cryptography Lecture Notes", California State University, East Bay, http://www.mcs.csueastbay.edu/~lertaul/
25. D. Wagner, "Cryptanalysis of an algebraic privacy homomorphism", In proceedings of the 6th information security conference (ISC03), Bristol, UK, October 2003.
26. William Stallings "Cryptography and Network Security", Third Edition, Chinese Remainder Theorem (CRT), pp. 245-247. Extended Euclid's Algorithm, pp. 119-220.
27. Jung Hee Cheon, Hyun Soon Nam, "A Cryptanalysis of the Original Domingo-Ferrer's Algebraic Privacy Homorphism", http://eprint.iacr.org/2003/221.pdf
28. William Stallings "Cryptography and Network Security", Third Edition, The RSA Algorithm, pp. 268-278.
29. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, Nov., 1976, pp. 644-654.
30. L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Comms of the ACM, v. 21-n.2, February 1978, pp. 120-126.
31. Yang Xiao. "Security in Sensor Networks", Auerbach Publications, 2007, pp. 275-290.
32. Dirk Westhoff, Joao Girao, Mithun Acharya. "Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution and routing adaptation". IEEE Transactions on Mobile Computing, October 2006.
33. R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms", in Foundations of Secure Computation, R. A. DeMillo et al., Eds. New-York: Academic Press, 1978, pp. 169-179.
34. Rakesh Agrawal., Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu: "Order-Preserving Encryption for Numeric Data". SIGMOD Conference 2004, pp 563-574.
35. J. Rissanen. "Stochastic complexity in statistical inquiry". World Scientific Publication, 1989.
36. L.Ertaul, Vaidehi, "Finding Minimum Optimal Path Securely Using Homomorphic Encryption Schemes in Computer Networks", The 2006 International Conference on Security & Management, SAM'06, June, Las Vegas.
37. P. Paillier. "Trapdooring Discrete Logarithms on Elliptic Curves over Rings". ASIACRYPT, pp 573–584, 2000.
38. Willian Stallings, "Cryptography and Network Security, Principles and Practices." Fourth Edition, Prentice Hall 2006, pp.312.
39. T. Okamoto and S. Uchiyama. "A New Public-Key Cryptosystem as Secure as Factoring". EUROCRYPT, pp 308–318, 1998.
40. GSL manual, http://www.gnu.org/software/gsl/manual/html_node/Random-Number-Distributions.html
41. Fork document, http://www.csl.mtu.edu/cs4411/www/NOTES/process/fork/create.html
42. W. Richard Stevens, "Unix Network Programming, Volume 2, Interprocess Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Message Queues, pp 75-126.
43. W. Richard Stevens, "Unix Network Programming, Volume 2, Inter process Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Shared memory, pp 325-342.

44. W. Richard Stevens, "Unix Network Programming, Volume 2, Interprocess Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Semaphore, pp 219-279.
45. GMP manual, "http://gmplib.org/manual/".
46. Cohen S psychological models of the role of social support in the etiology physical disease. Health Psychology 7 (1988) 269-297.
47. Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). http://www.cms.hhs.gov/hipaaGenInfo.
48. R. Agrawal, D. Asonov, M. Kantarcioglu and Y. Li. Sovereign Joins. In *ICDE 2006,* page 26. IEEE Computer Society, 2006.
49. F. Emekc¸ i, D. Agrawal, A. E. Abbadi and A. Gulbeden. Privacy Preserving Query Processing Using Third Parties. In *ICDE 2006,* page 27. IEEE Computer Society, 2006.
50. Dan Boneh, Ran Canetti, Shai Halevi and Jonathan Katz. Chosenciphertext security from identity-based encryption. SIAM J. Comput., 36(5):1301{1328, 2007.
51. M. Naor, B. Pinkas and R. Sumner. Privacy Preserving Auctions and Mechanism Design. In *Electronic Commerce 1999,* pages 129–139. ACM, 1999.
52. BRUCE SCHNEIER, "Applied cryptography – Protocols, Algorithms and Source Code in C" Second Edition.
53. Levent ertaul and Weimin Lu, "ECC Based Thresold Cryptography for Secure Data forwarding and Secure Key Exchange in MANET(I)." IFIP International federation for Information Processing – Networking 2005, LNCS 3462, pp 102- 113, 2005.
54. Mikhail J. Atallah, Keith B. Frikken, Marina Blanton, "Private Combinatorial Group Testing" *ASIACC'* 08, March 18-20, Tokyo, Japan 2008 ACM 978-1-59593-979-1/08/0003.
55. Human gemome project. http://genomics.energy.gov.
56. I. Damg°ard, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In Proceedings of the third Theory of Cryptography Conference, TCC 2006, volume 3876 of Lecture Notes in Computer Science, pages 285–304. Springer-Verlag, 2006.
57. *Dr. Abu Sayed Md. Latiful Hoque and Gahangir Hossain,* "PIR WITH PCACHE: ANEWPRIVATE INFORMATION RETRIEVAL PROTOCOL WITH IMPROVED PERFORMANCE" Malaysian Journal of Computer Science, Vol. 21(1), 2008.
58. Juan Ramón Troncoso-Pastoriza, Stefan Katzenbeisser Mehmet Celik," Privacy Preserving Error Resilient DNA Searching through Oblivious Automata" *CCS'07,* October 29–November 2, 2007, Alexandria, Virginia, USA.2007 ACM 978-1-59593-703-2/07/0011.
59. Zhiqiang Yang, Sheng Zhong, Rebecca N. Wright, "Towards Privacy Preserving Model Selection" Preproceedings version, PinKDD'07, August 12, 2007, San Jose, California, USA.
60. R. Agrawal and R. Srikant. Privacy preserving data mining. In *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 439–450. ACM Press, May 2000.
61. J. P. Prins, Z. Erkin, and R. L. Lagendijk, *"Research Article* Anonymous Fingerprinting with Robust QIM Watermarking Techniques" Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2007, Article ID 31340, 13 pages doi:10.1155/2007/31340.
62. C. Orlandi, A. Piva andM. Barni, *"Research Article* Oblivious Neural Network Computing via Homomorphic Encryption" Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2007, Article ID 37343, 11 Pages doi:10.1155/2007/37343.
63. Bart Goethals1, Sven Laur2, Helger Lipmaa2 and Taneli Mielik¨ainen1, "On Private Scalar Product Computation for Privacy-Preserving Data Mining" Helsinki University of Technology, Finland.
64. Thomas B. Pedersen, Erkay Savas and Yucel Saygin, "SECRET SHARING VS. ENCRYPTION-BASED TECHNIQUES FOR PRIVACYPRESERVING DATA MINING" Joint UNECE/Eurostat work session on statistical data confidentiality (Manchester, United Kingdom, 17-19 December 2007).
65. Mikhail J. Atallah, Florian Kerschbaum, "Secure and Private Sequence Comparisons "*WPES'03,* October 30, 2003, Washington, DC, USA. ACM \ 15811377 61/03/0010.
66. R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms" in R.A. DeMillo et al. eds., Foundations of Secure Computation (Academic Press, New York, 1978) 169-179.
67. E.F. Brickell and Y. Yacobi, "On privacy homomorphisms" in D. Chaum et al eds., Advances in Cryptology-Eurocrypt'87 (Springer, Berlin, 1988) 117- 125.
68. J. Domingo-Ferrer, "A new privacy homomorphism and applications" in Information Processing Letters, vol. 60, no. 5, pp. 277-282, Dec. 1996.
69. N. Ahituv, Y. Lapid and S. Neumann, "Processing encrypted data", Communications of the ACM, vol. 20, no. 9, pp. 777-780, Sep. 1987.
70. C. Ding, D. Pei and A. Salomaa, "Chinese remainder theorem," 1996.
71. J. Domingo-Ferrer and J. Herrera- Joancomarti, "A privacy homomorphism allowing field operations on encrypted data," *I Jornades de Matematica Discreta*

i Igorismica, Universitat Politecnica de Catalunya, 1998.
72. C. Negus, "Linux Bible: Boot Up to Fedora, KNOPPIX, Debian, SUSE, Ubuntu and 7 Other Distributions," 2006.
73. D. Westhoff, J. Girao and A. Sarma, "Security Solutions for Wireless Sensor Networks," *Nec Technical Journal*, vol. 1, 2006.
74. J. Girao, D. Westhoff, M. Schneider, N. E. C. E. Ltd, and G. Heidelberg, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," *Communications, 2005. ICC 2005. 2005 IEEE International Conference on,* vol. 5, 2005.
75. D. Integrity, P. Sakarindr and N. Ansari, "Security Services IN Group Communications OVER Wireless Infrastructure, Mobile Ad Hoc AND Wireless Sensor Networks," *IEEE Wireless Communications,* pp. 9, 2007.
76. Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, "Security Solutions for Wireless Sensor Networks" http://www.nec-display.com/products/model/lcd2180w _led/index.html
77. I. F. Blake, G. Seroussi and N. P. Smart. Elliptic curves in cryptography. Cambridge University Press, New York, NY, USA, 1999.
78. Alessandro Sorniotti, Laurent Gomez, Konrad Wrona and Lorenzo Odorico "Secure and Trusted innetwork Data Processing in Wireless Sensor Networks: a Survey" Journal of Information Assurance and Security 2 (2007) 189 –199.
79. Zhiqiang Yang1, Sheng Zhong2 and Rebecca N. Wright1, "Privacy- Preserving Queries on Encrypted Data⋆ In Proceedings of the 11th European Symposium On Research In Computer Security (Esorics), 2006.
80. **Mufutau Akinwande, "Advances in Homomorphic Cryptosystems"** *Journal of Universal Computer Science, vol. 15, no. 3 (2009), 506-522, 1/2/09 J.UCS.*
81. M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.
82. Brett Hemenawy and Rafail Ostrovsky, University of Michigan "On Homomorphic Encryption and Chosen-Cipher text Security" in the Proceedings of PKc 2012.
83. C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal,* vol. 28, pp. 656–715, 1949.
84. R. Rivest, L. Adleman and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.
85. R. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In Comm. of the ACM, 21:2, pages 120–126, 1978.
86. A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.
87. S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
88. T. ElGamal, "A prublic key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (CRYPTO '84), vol. 196 of Lecture Notes in Computer Science, pp. 10–18, Springer, New York, NY, USA, 1985.
89. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT'99), vol. 1592 of Lecture Notes in Computer Science, pp. 223–238, Springer, New York, NY, USA, 1999.
90. C. Fontaine, F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007, p.1-15, January 2007.
91. D. Micciancio and O. Regev. Post- Quantum Cryptography, chapter Lattice based Cryptography. Springer, 2008.
92. C. Gentry. Fully homomorphic encryption using ideal lattices. In Proc. of STOC, pages 169178. ACM, 2009.
93. N. P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. Lecture Notes in Computer Science, 2010, Volume 6056/2010, 420-443.
94. M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In Advances in Cryptology – Eurocrypt 2010, Springer LNCS 6110, 24–43, 2010.
95. Group Theory by "J S Milne" Version 3.12 April 9, 2012.
96. Brett Hemenway and Rafail Ostrovsky University of Michigan UCLA "On homomorphic Encryption and Chosen-Ciphertext Security".
97. Jibang Liu, Yung-Hsiang Lu, and Cheng-Kok Koh "Performance Analysis of Arithmetic Operations in Homomorphic Encryption".
98. Craig Gentry "A FULLY HOMOMORPHIC ENCRYPTION SCHEME".
99. Liangliang Xiao, Osbert Bastani, I-Ling Yen, "An Efficient Homomorphic Encryption Protocol for Multi-User Systems".

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Design and Implementation of Mobility for Virtual Private Network Users

By Md. Hashmathur Rehman

Abstract - Virtual Private Network framework provides Confidentiality, Integrity, Availability, Authentication and Anti- Replay services to the packets travelling through the shared medium like Internet. With the latest Advancement in the technology, Internet is available to the users thru all means like Wireless networks, GPRS, Satellite. When the VPN user roams or switches from one network to other, the IP address gets changed and VPN connection is tear down. The user has to again initiate the VPN connection whenever the network is switched. This paper present outcome of research project aimed at solving the mobility problems faced by roaming VPN users.

Keywords : *VPN, IPsec, AH, ESP, authentication algorithms, encryption algorithms.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Design and Implementation of Mobility for Virtual Private Network Users

Md. Hashmathur Rehman

Abstract - Virtual Private Network framework provides Confidentiality, Integrity, Availability, Authentication and Anti-Replay services to the packets travelling through the shared medium like Internet. With the latest Advancement in the technology, Internet is available to the users thru all means like Wireless networks, GPRS, Satellite. When the VPN user roams or switches from one network to other, the IP address gets changed and VPN connection is tear down. The user has to again initiate the VPN connection whenever the network is switched. This paper present outcome of research project aimed at solving the mobility problems faced by roaming VPN users.

Keywords : VPN, IPsec, AH, ESP, authentication algorithms, encryption algorithms.

I. Introduction

IP packets doesn't have any security when they travel through shared medium like internet. It needs security services like Confidentiality, Integrity, Authentication [6, 7]. Confidentiality is provided by encryption algorithms like DES, 3DES, AES. Integrity is provided by Hash Algorithms like MD5, SHA-1, SHA-2. Authentication is provided by preshared key mechanism or by using public key infrastructure like RSA (Rivest Shamir-Adleman) [8, 12]. These services are provided by maintaining shared state between the source and the destination of an IP datagram.

The protocol to establish this state dynamically is "Internet Key Exchange (IKE)" [1, 2]. IKE performs mutual authentication between two parties and establishes an IKE security association (SA) that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload [ESP] or Authentication Header [AH] and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry[1, 2].

II. VPNs, IKEv2

All IKE communications consist of pairs of messages: a request and are sponse. The pair is called an "exchange" and is sometimes called a "request/-response pair" [1]. The first exchanges of messages establishing an IKE SA are called the IKE_SA_INIT and IKE_AUTH exchanges; subsequent IKE exchanges are called the CREATE_CHILD_SA or INFORMATIONAL exchanges [2]. In the common case, there is a single IKE_SA_INIT exchange and a single IKE_AUTH exchange (a total of four messages) to establish the IKE SA and the first Child SA.

The first exchange of an IKE session, IKE_SA_INIT, negotiates security parameters for the IKE SA, sends nonces and sends Diffie-Hellman values [2].

The second exchange, IKE_AUTH, transmits identities, proves knowledge of the secrets corresponding to the two identities and sets up an SA for the first (and often only) AH or ESP Child SA (unless there is failure setting up the AH or ESP Child SA, in which case the IKE SA is still established without the Child SA) [2].

The types of subsequent exchanges are CREATE_CHILD_SA (which creates a Child SA) and INFORMATIONAL (which deletes an SA, reports error conditions, or does other housekeeping) [2]. Every request requires are sponse. An INFORMATIONAL request with no payloads (other than the empty Encrypted payload required by the syntax) is commonly used as a check for liveness. These subsequent exchanges cannot be used until the initial exchanges have completed [2].

a) Usage Scenarios

i. *Security Gateway to Security Gateway in Tunnel Mode*

IKE is used to negotiate ESP or AH SAs in a number of different scenarios, each with its own special requirements.

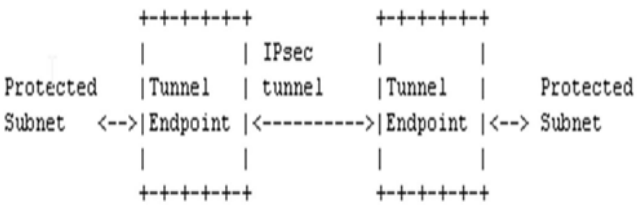


Figure 1 : Security Gateway to Security Gateway Tunnel

In this scenario, neither endpoint of the IP connection implements IPsec, but network nodes between them protect traffic for part of the way. Protection is transparent to the end points and depends on ordinary routing to send packets through the tunnel endpoints for processing. Each endpoint would announce the set of addresses "behind" it, and packets would be sent in tunnel mode where the inner IP header

Author : MobileIron Softwares India Pvt.
E-mail : ltdhashmath@gmail.com

would contain the IP addresses of the actual end points [2].

ii. *Endpoint-to-Endpoint Transport Mode*

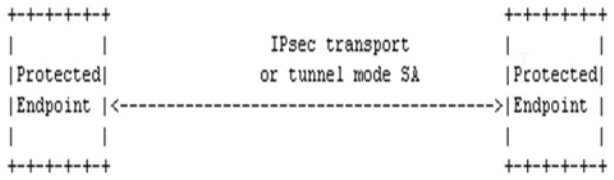


Figure 2 : Endpoint to Endpoint

In this scenario, both endpoints of the IP connection implement IPsec, as required of hosts in [IPSECARCH]. Transport mode will commonly be used with no inner IP header. A single pair of addresses will be negotiated for packets to be protected by this SA. The seend points MAY implement application-layer access controls based on the IPsec authenticated identities of the participants [2].

iii. *Endpoint to Security Gateway in Tunnel Mode*

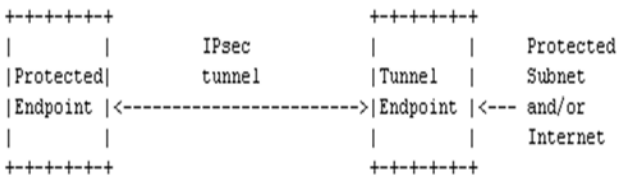


Figure 3 : Endpoint to Security Gateway Tunnel

In this scenario, a protected endpoint (typically a portable roaming computer) connects back to its corporate network through an IPsec-protected tunnel. The packets will use tunnel mode. On each packet from the protected endpoint, the outer IP header will contain the source IP address associated with its current location (i.e., the address that will get traffic routed to the endpoint directly), while the inner IP header will contain the source IP address assigned by the security gateway (i.e., the address that will get traffic routed to the security gateway for forwarding to the endpoint). The outer destination address will always be that of the security gateway while the inner destination address will be the ultimate destination for the packet [2].

b) Cryptographic Algorithm Negotiation

The payload type known as "SA" indicates a proposal for a set of choices of IPsec protocols (IKE, ESP, or AH) for the SA as well as cryptographic algorithms associated with each protocol [8, 9].

An SA payload consists of one or more proposals. Each proposal includes one protocol. Each protocol contains one or more transforms -- each specifying a cryptographic algorithm. Each transform contains zero or more attributes (attributes are needed only if the Transform ID does not completely specify the cryptographic algorithm) [2, 8].

This hierarchical structure was designed to efficiently encode proposals for cryptographic suites when the number of supported suites is large because multiple values are acceptable for multiple transforms. The responder MUST choose a single suite, which may be any subset of the SA proposal following the rules below [9].

Each proposal contains one protocol. If a proposal is accepted, the SA response MUST contain the same protocol. The responder MUST accept a single proposal or reject them all and return an error. The error is given in a notification of type NO_PROPOSAL_CHOSEN [2, 9].

Each IPsec protocol proposal contains one or more transforms. Each transform contains a Transform Type. The accepted cryptographic suite MUST contain exactly one transform of each type included in the proposal [2]. For example: if an ESP proposal includes transforms ENCR_3DES, ENCR_AES w/key size 128, ENCR_AES w/key size 256, AUTH_HMAC_MD5, and AUTH_HMAC_SHA, the accepted suite MUST contain one of the ENCR_ transforms and one of the AUTH_ transforms. Thus, six combinations are acceptable [2, 8].

If an initiator proposes both normal ciphers with integrity protection as well as combined-mode ciphers, then two proposals are needed. One of the proposals includes the normal ciphers with the integrity algorithms for them and the other proposal includes all the combined-mode ciphers without the integrity algorithms (because combined-mode ciphers are not allowed to have any integrity algorithm other than "none") [2, 8].

c) The Initial Exchanges

Communication using IKE always begins with IKE_SA_INIT and IKE_AUTH exchanges (known in IKEv1 as Phase 1). These initial exchanges normally consist of four messages, though in some scenarios that number can grow. All communications using IKE consist of request/ response pairs. We'll describe the base exchange first, followed by variations. The first pair of messages (IKE_SA_INIT) negotiates cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange [2].

The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates and establish the first Child SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated. All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the IKE_SA_INIT exchange [2].

All subsequent messages include an Encrypted payload, even if they are referred to in the text as

"empty". For the CREATE_CHILD_SA, IKE_AUTH, or INFORMATIONAL exchanges, the message following the header is encrypted and the message including the header is integrity protected using the cryptographic algorithms negotiated for the IKE SA [2].

Every IKE message contains a Message ID as part of its fixed header. This Message ID is used to match up requests and responses and to identify retransmissions of messages [2].

In the following descriptions, the payloads contained in the message are indicated by names as listed below.

Notation	Payload
AUTH	Authentication
CERT	Certificate
CERTREQ	Certificate Request
HDR	IKE header (not a payload)
IDi	Identification - Initiator
IDr	Identification - Responder
KE	Key Exchange
Ni, Nr	Nonce
SA	Security Association
TSi	Traffic Selector – Initiator
TSr	Traffic Selector – Responder
V	Vendor ID

The initial exchanges are as follows:

Initiator	Responder
HDR, SAi1, KEi, Ni -->	

HDR contains the Security Parameter Indexes (SPIs), version numbers, and flags of various sorts. The SAi1 payload states the cryptographic algorithms the initiator supports for the IKE SA. The KE payload sends the initiator's Diffie-Hellman value. Ni is the initiator's nonce [2].

Initiator	Responder
<-- HDR, SAr1, KEr, Nr, [CERTREQ]	

The responder chooses a cryptographic suite from the initiator's offered choices and expresses that choice in the SAr1 payload, completes the Diffie-Hellman exchange with the KEr payload, and sendsits nonce in the Nr payload [2].

d) The CREATE_CHILD_SA Exchange

The CREATE_CHILD_SA exchange is used to create new Child SAs and to rekey both IKE SAs and Child SAs. This exchange consists of a single request/response pair and some of its function was referred to as a Phase 2 exchange in IKEv1. It MAY be initiated by either end of the IKE SA after the initial exchanges are completed [2].

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term initiator refers to the endpoint initiating this exchange [2]. If a CREATE_CHILD_SA exchange includes a KEi payload, at least one of the SA offers MUST include the Diffie-Hellman group of the KEi. The Diffie-Hellman group of the Kei MUST be an element of the group the initiator expects the responder to accept (additional Diffie-Hellman groups can be proposed). If the responder selects a proposal using a different Diffie-Hellman group (other than NONE), the responder MUST reject the request and indicate its preferred Diffie-Hellman group in the INVALID_KE_PAYLOAD Notify payload. There are two octets of data associated with this notification: the accepted Diffie-Hellman group number in big endian order. In the case of such a rejection, the CREATE_CHILD_SA exchange fails, and the initiator will probably retry the exchange with a Diffie-Hellman proposal and KEi in the group that the responder gave in the INVALID_KE_PAYLOAD Notify payload [2].

The responder sends a NO_ADDITIONAL_SAS notification to indicate that a CREATE_CHILD_SA request is unacceptable because the responder is unwilling to accept any more Child SAs on this IKE SA. This notification can also be used to reject IKE SA rekey. Some minimal implementations may only accept a single Child SA setup in the context of an initial IKE exchange and reject any subsequent attempts to add more [2].

i. *Creating New Child SAs with the CREATE_CHILD_SA Exchange*

A Child SA may be created by sending a CREATE_CHILD_SA request. The CREATE_CHILD_SA request for creating a new Child SA is:

Initiator	Responder
HDR, SK {SA, Ni, [KEi], TSi, TSr} -->	

The initiator sends SA offer(s) in the SA payload, a nonce in the Ni payload, optionally a Diffie-Hellman value in the Kei payload, and the proposed Traffic Selectors for the proposed Child SA in the TSiand TSr payloads [2].

The CREATE_CHILD_SA response for creating a new Child SA is:

Initiator	Responder
<-- HDR, SK {SA, Nr, [KEr], TSi, TSr}	

The responder replies (using the same Message ID to respond) with the accepted offer in an SA payload, and a Diffie-Hellman value in the KEr

payload if KEi was included in the request and the selected cryptographic suite includes that group [2].

The Traffic Selectors for traffic to be sent on that SA are specified in the TS payloads in the response, which may be a subset of what the initiator of the Child SA proposed [2].

III. IKEv2 Mobility (MOBIKE)

IKEv2 is used for performing mutual authentication, as well as establishing and maintaining IPsec Security Associations (SAs) [2, 3]. In the base IKEv2 protocol [IKEv2], the IKE SAs and tunnel mode IPsec SAs are created implicitly between the IP addresses that are used when the IKE_SA is established. These IP addresses are then used as the outer (tunnel header) addresses for tunnel mode IPsec packets (transport mode IPsec SAs are beyond the scope of this document). Currently, it is not possible to change these addresses after the IKE_SA has been created [3].

There are scenarios where these IP addresses might change. One example is mobility: a host changes its point of network attachment and receives a new IP address [3]. Another example is a multi-homing host that would like to change to a different interface if, for instance, the currently used interface stops working for some reason.

The main scenario for MOBIKE is enabling a remote access VPN user to move from one address to another without reestablishing all security associations with the VPN gateway [3]. For instance, a user could start from fixed Ethernet in the office and then disconnect the laptop and move to the office's wireless LAN. When the user leaves the office, the laptop could start using General Packet Radio Service (GPRS); when the user arrives home, the laptop could switch to the home wireless LAN. MOBIKE updates only the outer (tunnel header) addresses of IPsec SAs, and the addresses and other traffic selectors used inside the tunnel stay unchanged. Thus, mobility can be(mostly) invisible to applications and their connections using the VPN [2, 3].

MOBIKE allows both parties to have several addresses and there are up to N*M pairs of IP addresses that could potentially be used. MOBIKE solves this problem by taking a simple approach: the party that initiated the IKE_SA (the "client" in a remote access VPN scenario) is responsible for deciding which address pair is used for the IPsec SAs and for collecting the information it needs to make this decision (such as determining which address pairs work or do not work). The other party (the "gateway" in a remote access VPN scenario) simply tells the initiator what addresses it has, but does not update the IPsec SAs until it receives a message from the initiator to do so.

This approach applies to the addresses in the IPsec SAs; in the IKE_SA case, the exchange initiator can decide which addresses are used [3].

A simple MOBIKE exchange in a mobile scenario is illustrated below.The notation is based on [IKEv2] [3].

Step 1 : Is the normal IKE_INIT exchange [2, 3].
Step 2 : The peers inform each other that they support MOBIKE [3].
Step 3 : The initiator notices a change in its own address and informs the responder about this by sending an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification [3]. The request is sent using the new IP address. At this point, it also starts to use the new address as a source address in its own outgoing ESP traffic. Upon receiving the UPDATE_SA_ADDRESSES notification, the responder records the new address and, if it is required by policy, performs a return rout ability check of the address [3].

When this check (step 4) completes, the responder starts to use the new address as the destination for its outgoing ESP traffic.

a) *Protocol Exchanges*

i. *Initial IKE Exchange*

The initiator is responsible for finding a working pair of addresses so that the initial IKE exchange can be carried out. Any information from MOBIKE extensions will only be available later, when the exchange has progressed far enough. Exactly how the addresses used for the initial exchange are discovered is beyond the scope of this specification; typical sources of information include local configuration and DNS [3]. If either or both of the peers have multiple addresses, some combinations may not work. Thus, the initiator SHOULD try various source and destination address combinations when retransmitting the IKE_SA_INIT request [3].

ii. *Signaling Support for MOBIKE*

Implementations that wish to use MOBIKE for a particular IKE_SA MUST include a MOBIKE_SUPPORTED notification in the IKE_AUTH exchange (in case of multiple IKE_AUTH exchanges, in the message containing the SA payload) [3].

iii. *Initial Tunnel Header Addresses*

When an IPsec SA is created, the tunnel header IP addresses (and port, if doing UDP encapsulation) are taken from the IKE_SA, not the IP header of the IKEv2 message requesting the IPsec SA. The addresses in the IKE_SA are initialized from the IP header of the first IKE_AUTH request [3].

iv. *Additional Addresses*

Both the initiator and responder MAY include one or more ADDITIONAL_IP4_ADDRESS and/or ADDITIONAL_IP6_ADDRESS notifications in the IKE_AUTH exchange (in case of multiple IKE_AUTH exch-

anges, in the message containing the SA payload). Here "ADDITIONAL_*_ADDRESS" means either an ADDITIONAL_IP4_ADDRESS or an ADDITIONAL_IP 6_ADDRESS notification [3].

v. *Changing Addresses in IPsec SAs*

In MOBIKE, the initiator decides what addresses are used in the IPsec SAs. That is, the responder does not normally update any IPsec SAs without receiving an explicit UPDATE_SA_ADDRESSES request from the initiator. (As described below, the responder can, however, update the IKE_SA in some circumstances.) [3]

IV. Conclusions

The main goals of this research project are to maintain the security offered by usual IKEv2 procedures and to counter mobility-related threats in an appropriate manner. This section describes new security considerations introduced by MOBIKE.

1. Traffic Selector Authorization.
2. Traffic Redirection and Hijacking.
3. IPsec Payload Protection.
4. Denial-of-Service Attacks against Third Parties.
5. Spoofing Network Connectivity Indications.
6. Performance tuning for support to Mobile devices like Smartphones, IPADS, Tablets.

References Références Referencias

1. IKEv1, The Internet Key Exchange (IKE) RFC 2409, available athttp://tools.ietf.org/html/rfc2409
2. Internet Key Exchange Protocol Version 2 (IKEv2) IKEv2, RFC 5996, available at https://tools.ietf.org/html/rfc5996
3. IKEv2 Mobility and Multihoming Protocol (MOBIKE), http://tools.ietf.org/html/rfc4555
4. S. Frankel, et al. Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-77, available at http://www.nist.gov
5. A. Uskov, “Information Security of Mobile VPN: Conceptual Models and Design Methodology”, Proc. 2012 IEEE international conference on Electro/Information Technology EIT-2012. Indianapolis, IN; catalog number: CFP12EITCDR; ISBN: 978-1-4673-0818-2; ISSN: 2154-0373.
6. J. Carmouche, IPsec Virtual Private Network Fundamentals. Indianapolis, IN: Cisco Press, 2007.
7. V. Bollapragada, M. Khalid, S. Wainner, IPSec VPN Design. Indianapolis, IN: Cisco Press, 2005.
8. B. Schneider, Applied Cryptography: Protocols, Algorithms, and Source Code in C. Indianapolis, IN: Wiley, 1996.
9. N. Ferguson, B. Schneider, Practical Cryptography. Indianapolis, IN: Wiley, 2003.
10. N. Ferguson, B. Schneider, T. Kohno, Cryptography Engineering. Indianapolis, IN: Wiley, 2010.
11. IKEv2 Parameters, RFC4306, available at http://www.iana.org/assignments/ikev2-parameters
12. RSA Security, available at http://www.rsa.com

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Increase the Alive Nodes based on the Cluster Head Selection Algorithm for Heterogeneous Wireless Sensor Networks

By C. Divya, N. Krishnan & A. Petchiammal
Manonmaniam Sundaranar University Tirunelveli, India

Abstract - The use of Wireless Sensor Networks (WSNs) is estimated to bring enormous changes in data gathering, processing and distribution for different environments and applications. However, a WSN is a powerful controlled system, since nodes run on limited power batteries. Prolong the lifetime of sensor networks depends on efficient management of sensing node of energy. Hierarchical routing protocols are best known in regard to energy efficient. By using a clustering technique hierarchical routing protocol greatly minimize the energy consumed in collecting and distributing the data. The proposed protocol focuses on reducing the energy consumption and increasing the energy efficiency and also increasing the number of alive nodes of wireless sensor networks better than exiting protocol.

Keywords : *wireless sensor network, LEACH protocol, new protocol, energy consumption, energy efficiency.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Increase the Alive Nodes based on the Cluster Head Selection Algorithm for Heterogeneous Wireless Sensor Networks

C. Divya [α], N. Krishnan [σ] & A. Petchiammal [ρ]

Abstract - The use of Wireless Sensor Networks (WSNs) is estimated to bring enormous changes in data gathering, processing and distribution for different environments and applications. However, a WSN is a powerful controlled system, since nodes run on limited power batteries. Prolong the lifetime of sensor networks depends on efficient management of sensing node of energy. Hierarchical routing protocols are best known in regard to energy efficient. By using a clustering technique hierarchical routing protocol greatly minimize the energy consumed in collecting and distributing the data. The proposed protocol focuses on reducing the energy consumption and increasing the energy efficiency and also increasing the number of alive nodes of wireless sensor networks better than exiting protocol.

Keywords : wireless sensor network, LEACH protocol, new protocol, energy consumption, energy efficiency.

I. Introduction

The Wireless Sensor Networks (WSN) [1, 2, and3] is a broadcast network consists of a large number of sensor nodes that are limited in energy, processing power, storage and sensing ability. The WSN based on routing techniques that handles more complex functions. The energy of nodes is the most important consideration among them because the lifetime of Wireless Sensor Networks is limited by the energy of the nodes. Thus, a network of these sensors gives increase to more robust, reliable and accurate network.

The WSN is used the two types of networks homogeneous and heterogeneous. The homogeneous mixture is a mixture where the components that make up the mixture are uniformly distributed throughout the mixture. The heterogeneous mixture is a mixture where the components of the mixture are not uniform or have localized regions with different properties, but heterogeneous networks are more efficient than the homogeneous network in WSN.

LEACH (Low-Energy Adaptive Clustering Hierarchy) [4] is a clustering-based protocol and one of the first hierarchical routing approaches for sensor networks that utilizes the randomized rotation of local cluster base stations to evenly distribute the energy load within the network of sensors. In LEACH, the cluster head (CH) nodes reduce the data arriving from nodes that belong to the particular cluster, and send an aggregated data to the base station in order to reduce the amount of information that must be transmitted to the base station. WSN is considered to be a dynamic clustering method. The dynamic is changing the network parameters.

We use the concept of heterogeneity and tried to improve the LEACH [5] algorithm. In this approach, cluster head gets the data from nodes of the cluster and aggregate the data before sending it to the base station. In each round cluster head rotates and consumes the same energy, hence it utilizes the uniform energy distribution for the whole network. The LEACH protocol follows the concept of nodes homogeneity, which means that entire nodes have same initial energy. But practically it is visible that the network is not pure homogeneous. The heterogeneity, which means some of the nodes of the sensor network are equipped with additional initial energy, this type of sensor network is called heterogeneous wireless sensor network. This protocol of LEACH does not give good result so we have to provide some modification in the existing protocol.

LEACH is a cluster based routing protocol and one of the hierarchical based routing [6] protocols. Hierarchical based routing is to efficiently maintain the energy consumption of sensor nodes and communication between a number of nodes within a particular time and by performing data aggregation and data fusion. Data fusion helps to reduce the amount of data transmitted between sensor nodes and the base station.

The new proposed protocol is an energy efficient communication protocol for WSN. The communication takes place between all the cluster members and cluster heads. The cluster heads can perform data aggregation for communicating to the Base Station. The number of transmission is reduced from cluster to base station known as data aggregation. The new protocol can achieve energy efficiency, reduces energy consumption and increasing the number of a live nodes in every round than existing algorithms.

Authors α σ ρ : Center for Information technology and Engineering Manonmaniam Sundaranar University Tirunelveli, Tamil Nadu, India.
E-mails : divyame@gmail.com, petchiammalmtech17@gmail.com

The paper is organized as follows: Section II describes the assumptions used for the related work. In Section III describes the design of LEACH protocol and new proposed protocol in detail. The simulation result is discussed in Section IV. Finally conclusions made in Section V.

II. Related Work

WSN involves so many clustering techniques such as LEACH [7, 8], EEAP [9], En-LEACH [10], EERR [11], EAPHRN [12], and I-LEACH [13] for balancing the energy consumption, increase the energy efficiency and increase the lifetime of the sensor network. LEACH (Low Energy Adaptive Clustering Hierarchy) [7] is one of the important clusters based structures, in wireless sensor networks. LEACH uses a TDMA technique based MAC protocol, and in order to maintain balanced energy consumption. TDMA (Time Division Multiple Access) is a more flexible scheme which comprises all technologies that allocate certain time slots for particular communication means that the receiver can stay at the same frequency the whole time. LEACH protocol is used to reduce the energy consumption of the network resource in each round.

LEACH protocols [8] highly affect the performance of wireless sensor networks by an even distribution of energy load and decreasing their energy consumption and prolonging their lifetime. Thus, designing energy efficient protocols is important for prolonging the lifetime of wireless sensor networks. Leach-Heterogeneous System provides better energy efficiency and increasing the lifetime of the wireless sensor networks than homogeneous networks.

Energy-Efficient Adaptive Protocol for Clustered Wireless Sensor Networks (EEAP) [9] is used to increase the lifetime of the sensor networks by balancing the energy consumption of the nodes. EEAP makes the high residual energy node to become a cluster-head. The elector nodes are used to collect the energy information of the neighbor sensor nodes and select the cluster-heads and increase the energy efficiency.

In En-LEACH [10], all cluster members are reserved informed about the cluster head, since the probability of breakdowns of cluster-head is high during the data transmission phase. En-LEACH is more effective; producing the information about the nodes are monitoring in an energy-efficient. En-LEACH is able to handle non-uniform energy distribution of sensor nodes which is an important characteristic of a dynamic sensor networks.

EERR (Energy Efficient and Reliable Routing protocol) [11] is an extension of leach where the cluster head is called headset. The headset consist the number of nodes and each node will be acting like a cluster head in a particular time interval. Two types of phases. In the election phase the cluster head is selected on a random basis.CH node is an advertising message to all nodes in the network using a CSMA MAC protocol. Each node transmits a unite request message to the CH as an acknowledgment. Using this CH forms a headset. The headset is followed by TDMA schedule and transmits this schedule to the nodes in the cluster. In this data transfer phase, all the non-cluster head nodes will collect the information and transmit it into the headset. Then the headset transmits or sends it into the base station. The next new round all the nodes are taken as a normal node and the process will continue further.

EAPHRN (Energy aware PEGASIS based Hierarchical routing protocol) [12] is a hierarchical chain based routing protocol. In EAPHRN, the nodes can select randomly forms a group of possible nodes but within the distance threshold DT. In EAPHRN divided into two phases. In the first phase chain set up, each node must be calculate the local DT (LDT). It is an average distance between the node and the neighboring node in the network. LDT threshold is computed, after that, the node sends to the BS. BS collects all the LDT from the number of nodes and calculated the DT. Then it sends the DT to the number of nodes in the WSN to start forming the chain. Finally, when the chain formed, choosing a chain leader is based on the leader is a closest node to the BS. Once chain leader received the data it aggregates and sends it in to BS.

I-LEACH (Improved LEACH) [13] is enhanced from the leach protocol. I-leach solves the problem of node heterogeneity. In I-leach the selection of cluster head is based on the residual energy rather than probability. If the nodes have different initial energy levels instead of uniform initial energy level, they selection of cluster head can be prepared effectively. I-Leach each node will have a CH in their neighborhood. It improves the lifetime of the network.

III. Protocol Performance

a) LEACH Protocol

Low-energy adaptive clustering hierarchy (LEACH) is one of the most popular hierarchical routing algorithms for wireless sensor networks. Is protocol architecture for micro sensor networks that combine the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and production cost.

Calculate the distance (d_0) by using energy per bit (E_{fs}) divide energy per area (E_{mp}).

$$d_0 = \frac{E_{fs}}{E_{mp}} \quad (1)$$

i. *Cluster Heads Selection Algorithm*

$$T(n) = \begin{cases} \dfrac{P}{\left(1-P*mod\left(r,round\left(1/P\right)\right)\right)} & n \in G \\ 0 & Otherwise \end{cases} \quad (2)$$

With P is the cluster-head probability, r is the number of the round and G is the set of node. This algorithm ensures that every node becomes a cluster-head exactly once within rounds. Although the randomization of electing cluster head nodes can distribute the load among the network. Cluster heads have changed randomly over time in order to balance the energy dissipation of nodes. This decision is made by the nodes are choosing a randomly the values of each node between 0 and 1. If random $< T(n)$, means the sensor node becomes the cluster-head, otherwise it is a cluster member.

a. *Minimum Distance*

Find the minimum distance for the election of an associated cluster head for by m_d.

In LEACH we need to find the minimum distance in order to send data from the base station to cluster head.

$$m_d = \sqrt{(XR(i)-C(c).xd)^2+(YR(i)-C(c).yd)^2} \quad (3)$$

If the minimum distance greater than the initial energy

$$E_d = E_d-(ETX*(cpl)+E_{mp}*cpl*(m_d{}^4) \quad (4)$$

In the Eq. (4) E_d is the initial energy of each node. The ETX is the transmitted the energy. Length of packet (cpl) sends the packet between the base stations to the cluster head.

Length of packet (*pl)* sends the packet between the base station to cluster head.

$$E_d = E_d-(ETX*(pl)+E_{mp}*pl*(m_d{}^4) \quad (5)$$

Two types of transmitting amplifier, first one E_{fs} and second one E_{mp}. E_{fs} is the energy per bit and E_{mp} is the energy per area.

If the minimum distance less than the initial energy

$$E_d = E_d-(ETX*(cpl)+E_{fs}*cpl*(m_d{}^2) \quad (6)$$

$$E_d = E_d-(ETX*(pl)+E_{mp}*pl*(m_d{}^2) \quad (7)$$

b) New Protocol

The main aim of the new protocol is the hierarchical routing is to efficiently maintain the energy consumption and increasing the energy efficiency of sensor nodes by performing data aggregation and data fusion in order to decrease the number of transmitted between the cluster head and the base station. All sensor nodes are identical and charged with the same amount of initial energy. The new protocol can achieve energy efficiency, reduces energy consumption and increasing the number of alive nodes in each on every round than existing algorithms.

Protocol based dynamic clustering method. Dynamic routing allows routing is to change the possible routes. In case of wireless sensor networks dynamic routing is employed because nodes may frequently change their position and die at any moment.

i. *Cluster Head Selection Algorithm*

In the Eq. (8), *p* is the percentage of cluster heads over all nodes in the network, i.e., the probability (0.05) that a node is selected as a cluster head; r the number of rounds of selection; and G is the set of nodes that are not selected in round 1/p. E_0 is the initial energy (0.5 J) divided by the number of nodes and multiply the X is the optimal cluster head number. As we can see here, the selection of cluster heads is totally random.

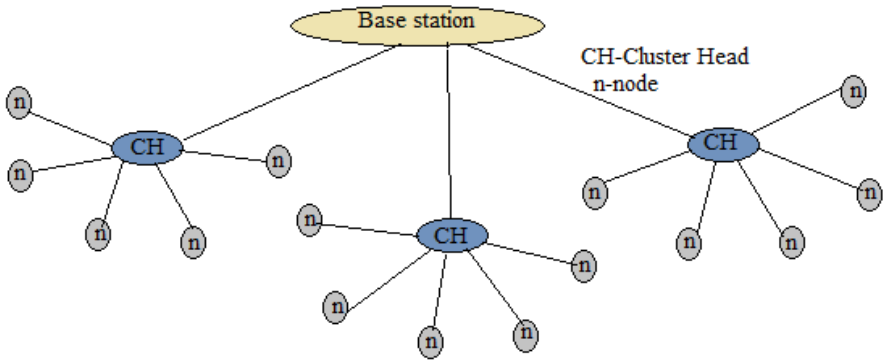
$$T(n) = \frac{P}{\left(1-P*mod\left(r,round\left(1/P\right)\right)\right)} - \left(E_0/(n*X)\right) \quad (8)$$

$$X = \left(\frac{n}{2}*\frac{22}{7}*d_0*sqrt\left(M/d_{bs}\right)\right) \quad (9)$$

Where *X* is the optimal cluster head number, n is the total number of sensor nodes, M (10) is the length of nodes distributing fields, d_{bs} (30) *is* the distance between the nodes and the Base Station.

Fig. 1 First select particular node, that node is known as cluster head and joining the number of nodes with cluster head. Number of individual nodes are connected is known as clustering. All clusters are having one cluster head which performs data collection and data fusion. Clustering is the method by which sensor nodes in a network organize themselves into hierarchical structures. Cluster head provides data communication and data aggregation also. It is the number of nodes that sends data to the sink directly after aggregating the data.

Figure 1 : Communication between all the nodes in Cluster Head and Cluster Head for Base Station



Each on every node sends the data to its own cluster head. There are two steps in Data transmission. Firstly, data are transmitted to cluster head nodes and second step the data aggregation takes place from cluster head to base station.

a. *Minimum Distance*

Minimum Distance for only nodes:

The minimum distance is called based on Eq. (3)

Minimum distance from cluster head:

$$E_d = \begin{cases} E_d - \left(ETX + E_{mp} * {m_d}^4\right) & m_d > do \\ E_d - \left(ETX + E_{fs} * {m_d}^4\right) & otherwise \end{cases} \quad (10)$$

In the Eq. (4) E_d is the initial energy of each node. The *ETX* is the transmit energy (5×10^{-8}). Two types of transmitting amplifier, first one E_{fs} and second one E_{mp}. E_{fs} Is the energy per bit (10^{-11}) and E_{mp} is the energy per area (1.3×10^{-15}). m_d Is the minimum distance from cluster head. C_{md} Is the initial energy for a minimum distance of the cluster. Two types energy (*ETX, ERX*), *ETX* and *RTX* (5×10^{-8}) are the transmit energy and receive energy, In Eq.11 using the receive energy. l Is the length of the packet (6400) are multiplied when the minimum distance greater than zero otherwise using cl is the length of control packet (200), the initial energy is divided by residual energy. They are using transmit the packet between cluster head to the base station.

$$C_{md} = \begin{cases} (ERX * l * m_d * Eo/res) & (m_d > 0) \\ (ERX * cl * m_d * Eo/res) & otherwise \end{cases} \quad (11)$$

In Eq. 12 using the receive energy (ERX), the receive energy is 5×10^{-8} and energy per area are multiplied when the minimum distance is greater than distance otherwise using the energy per bit for increase the number of alive nodes in each round.

$$C_{md} = \begin{cases} \left(ERX * E_{mp} * m_d * Eo/res\right) & (m_d > d_0) \\ \left(ERX * E_{fs} * m_d * Eo/res\right) & otherwise \end{cases} \quad (12)$$

IV. Simulation Result

The performance of new protocol was analyzed using MATLAB. The number of rounds(r=10,000) is considered in X axis and the number of alive nodes (n=100) in Y axis.

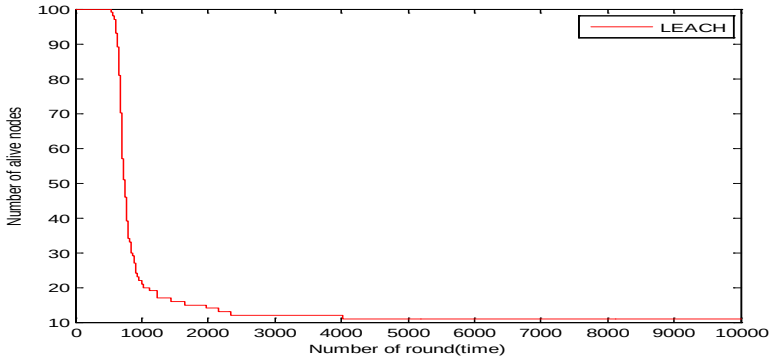


Figure 2 : LEACH Protocol

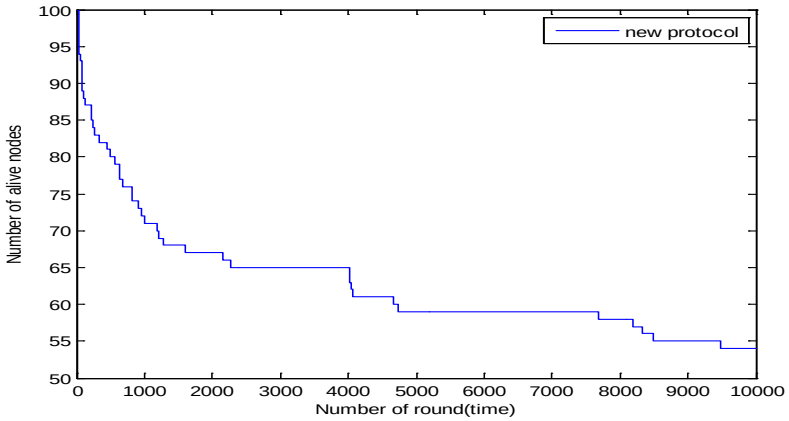


Figure 3 : New Protocol

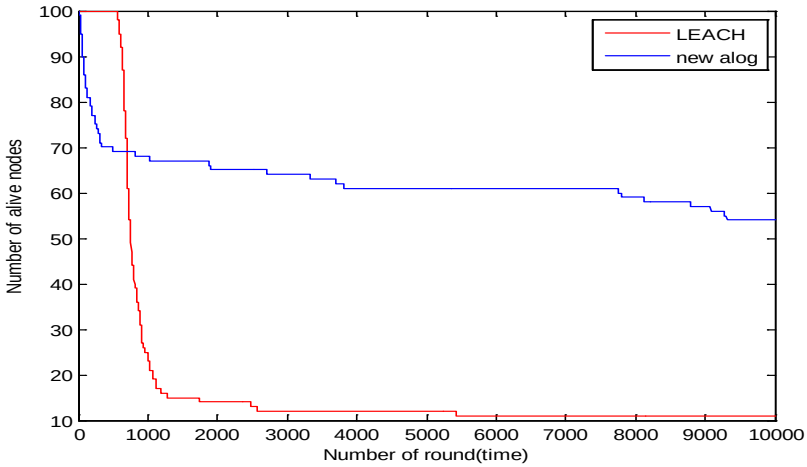


Figure 4 : Comparative analysis of LEACH and new protocol

Figure 2 shows the energy efficiency of the LEACH algorithm. Rounds increases from 0 to 10,000. The number of alive nodes was calculated for each round in order to find the energy efficiency of the network. The existing algorithm increasing the number of alive is 20 percentages. Figure 3 shows the energy efficiency of the new algorithm. Rounds increases from 0 to 10,000. The number of alive nodes was calculated for each round in order to find the energy efficiency of the networks. In the new protocol of heterogeneous system is number of alive nodes is increased near to 60% than the leach heterogeneous system and lifetime of the networks also increased. From the comparative analysis of figure 4, we analyze that the number of alive nodes is increasing in newer protocol than LEACH protocol.

V. Conclusion

LEACH protocol is one of the routing protocols based on clustering algorithm to calculate the energy efficiency of the network. A new protocol was proposed based on existing LEACH protocol to save the energy of the network. Energy efficiency was analyzed by calculating the number of alive nodes in the network by considering the number of rounds. The performance analysis using MATLAB shows that the number of alive nodes is increasing in each round than exiting algorithm. Thus the new protocol is suitable to save the energy of the network, increasing the number of alive nodes and energy efficient.

References Références Referencias

1. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, August 2002.
2. I.F. Akyildiz, W.J. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.
3. K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks 3 (3) (2005) 325–349.
4. Baiping Li, Xiaoqin Zhang "Research and Improvement of LEACH Protocol for Wireless Sensor Network" International Conference on Information Engineering *Lecture Notes in Information Technology, Vol. 25 -2012.*
5. W. R. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "Energy efficient Communication protocol for wireless Microsensor networks," *Proceedings of 33rd Hawaii International Conference on System Sciences (HICSS)*, 2000.
6. W.R. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.
7. Mortaza Fahimi Khaton Abad, Mohammad Ali Jabraeil Jamali "Modify LEACH Algorithm for Wireless Sensor Network" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011.
8. R. Saravanakumar, S. G. Susila, J. Raja "Energy Efficient Homogeneous and Heterogeneous System for Wireless Sensor Networks" *International Journal of Computer Applications (0975 – 8887) Volume 17– No.4, March 2011.*
9. K. Padmanabhan , Dr. P. Kamalakkannan "Energy Efficient Adaptive Protocol for Clustered Wireless Sensor Networks" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011 ISSN (Online): 1694-0814
10. Mr. Halke Rajesh 1, Mrs. Kulkarni V. A." Design of Enhanced LEACH Routing Protocol for Wireless Sensor Network" *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN: 2278-2834, ISBN: 2278-8735, PP: 07-12*
11. Padmavathy, T. V, Chitra M "EERR: Performance Evaluation of Energy Efficient and Reliable routing protocol for wireless sensor networks" Data management and network control in wireless networks (SICN), Volume(0), Issue(0): 2011.
12. Hasan Al. Hasan, Mohammad qatawneh, Azzam Sleit, Wesam Almobaideen "EAPHRN: Energy aware PEGASIS Based Hierarchical Routing protocol for wireless sensor networks" Journal of American science, 2011.
13. Naveen kumar, Mrs. Jasbir kaur "Improved Leach Protocol for Wireless sensor Networks", IEEE, 2011.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

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.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

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

A

Attenuates · 1

B

Botnet · 12, 13, 14, 15, 16, 18
Breadcrumbs · 19, 20, 21, 22, 23, 24

C

Cipher · 27, 28, 36, 37

D

Deciphers · 28
Dissipation · 72

E

Eavesdroppers · 48
Elgamal · 34, 36, 37, 38, 39, 41

H

Homomorphic · 27, 34, 36, 40, 41, 44

M

Menezes · 34, 42
Metaphorical · 55

O

Obesity · 54

P

Phishing · 12, 56
Preexisting · 31

R

Relying · 31, 32
Repudiation · 29, 32

S

Stochastic · 42

T

Tcpdump · 14
Tedious · 19, 20, 21, 22, 23, 24, 25, 55
Trentino · 41

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