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

Global Journal

of Computer Science and Technology : E

Network, Web & Security

DISCOVERING THOUGHTS AND INVENTING FUTURE

Highlights

Coverage of Wireless Sensors

Adaptive Hybrid Routing Topology

Data Provenance Verification

Mobile Application Development

Computer Server Farm

Volume 12 | Issue 15 | Version 1.0

ENG

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

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

Volume 12 Issue 15 (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: Global Association of Research

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.)

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 15 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Smart Connect Using Cellular Technology

By Ms. Priyanka V. Kampasi & Y.C. Kulkarni

Bharati Vidyapeeth's College of Engineering/IT, Pune, India

Abstract - Technical developments in computer hardware and software make it possible to introduce automation into virtually all aspects of human-machine systems. Automation has made Software applications much more efficient to use. This paper proposes that automation can be applied to desktop sharing in which a system can operate automatically anywhere in the world using GSM technology & VIRTUAL LAN concept.

The proposed system will be used to make the purpose of data access simpler, keeping in mind the needs of the IT industries. Through this system, automated desktop sharing can be implemented with effective cause. Today's desktop conferencing and groupware software often assume a serial work model in which information (pictures, documents, presentations) are prepared by one person and then disseminated to others for comments, revision, or review. However, many types of collaborative work are much more parallel, with many people viewing, updating, and adding information concurrently across cross-platform display sharing between Mac OS, Windows, and UNIX operating systems. The current EMSL Televiewer prototype supports display sharing of application windows, screen regions, and desktops. This system proposes enhancements to the EMSL Televiewer that will provide collaborative annotations over the display, shared mouse cursors, pointer, high performance data compression, and session recording capabilities. When completed, the EMSL Televiewer will provide researchers and the scientific community a powerful tool that can by itself open up many new avenues for collaboration and will fit well with other tools to provide a comprehensive collaborative environment.

Keywords : Cell Phone, Desktop Sharing, Encryption, GSM, Microcontroller.

GJCST-E Classification : C.2.1

SMART CONNECT USING CELLULAR TECHNOLOGY

Strictly as per the compliance and regulations of:

OPEN ASSOCIATION OF RESEARCH SOCIETY, USA
RESEARCH | DIVERSITY | ETHICS

Smart Connect Using Cellular Technology

Ms. Priyanka V. Kampasi & Y.C. Kulkarni

Abstract - Technical developments in computer hardware and software make it possible to introduce automation into virtually all aspects of human-machine systems. Automation has made Software applications much more efficient to use. This paper proposes that automation can be applied to desktop sharing in which a system can operate automatically anywhere in the world using GSM technology & VIRTUAL LAN concept.

The proposed system will be used to make the purpose of data access simpler, keeping in mind the needs of the IT industries. Through this system, automated desktop sharing can be implemented with effective cause. Today's desktop conferencing and groupware software often assume a serial work model in which information (pictures, documents, presentations) are prepared by one person and then disseminated to others for comments, revision, or review. However, many types of collaborative work are much more parallel, with many people viewing, updating, and adding information concurrently across cross-platform display sharing between Mac OS, Windows, and UNIX operating systems. The current EMSL Televiewer prototype supports display sharing of application windows, screen regions, and desktops. This system proposes enhancements to the EMSL Televiewer that will provide collaborative annotations over the display, shared mouse cursors, pointer, high performance data compression, and session recording capabilities. When completed, the EMSL Televiewer will provide researchers and the scientific community a powerful tool that can by itself open up many new avenues for collaboration and will fit well with other tools to provide a comprehensive collaborative environment.

Keywords : Cell Phone, Desktop Sharing, Encryption, GSM, Microcontroller.

I. Introduction

The concept of Desktop Sharing has revolutionized the work of IT professionals immensely. While sitting at home or while roaming, an IT professional can work on his office computer anytime. The Computer system in the office can be accessed by the employee anywhere. Yes, of Course there are security considerations that must be met. That is, the authenticity of the person requesting access to the workplace computer. Earlier even though a person could remotely access his/her office computer but still he/she required a desktop computer or a laptop. The Goal of designing this application is for the benefit of industry people by allowing them multi-sharing of the computer screen for their assignments through cellular technology like a Cell Phone. It requires a PC with a modem setup. The Computer/laptop contains important data or information. This information can be accessed by the user anywhere anytime through her mobile phone. The Cell Phone must be Internet enabled. When a request is send by the cell phone to the respective modem which is received using the GSM system, it shall respond back by sending an acknowledgment message asking password so as to confirm that an authentic user has made the request.

As soon as the correct password is received as a response to the request, the system shall generate 4-digit conformation code for establishing the connectivity. As soon as the system is connected, the data transfer can take place. For providing security to the data transmission, SHA-1 algorithm is used.

The system is basically focused for those people who travel around the globe and need to be consistently connected to their workplace or home at the same time.

The proposed system has a great potential and it will benefit the masses for a long time.

Everybody these days possesses a Mobile Phone. As it is small in size and portable, it become a smarter choice for accessing the remote desktop than a PC or a laptop. This paper proposes the use of Mobile Phones (equipped with Internet features) by the IT professionals to access their office computers after proper authentication check.

The overall system will require hardware components like a Modem, Microcontroller, Microprocessor and a USB Port to accomplish this task. For secure transmission of data between the cellular device and the PC, encryption algorithm (SHA 1) will be used.

Apart from this if ROBOT APIs are used then we can use our Mobile phone as a remote control for switching on or off the lights, adjusting the thermostat of our AC. It could also be used for indicating the temperature in high temperature zones like Nuclear Reactors.

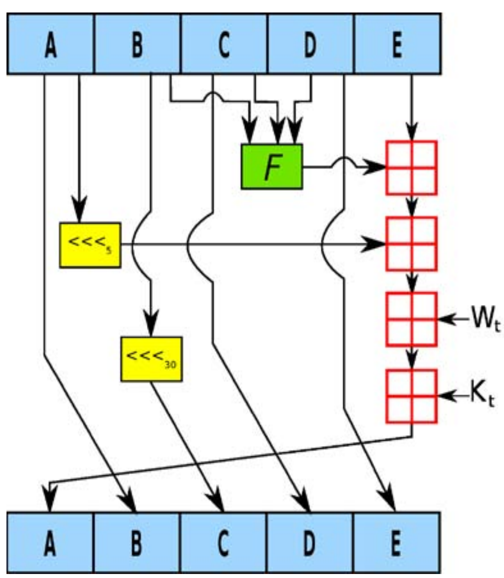
The whole application is divided into modules according to their functionalities. The output of one module is input for the next module. Intended Audience and Reading Suggestions This document is intended for the persons in the following categories Students doing Graduation in Computers. Internal and External guide.

Most of the industries need it for their project development.

Author : Bharati Vidyapeeth's College of Engineering/IT, Pune, India.
E-mails : kampasipriyanka@gmail.com, yckulkarni@yahoo.com

a) The SHA-1 hash function

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design. The original specification of the algorithm was published in 1993 as the *Secure Hash Standard*, FIPS PUB 180, by US government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as *SHA-0*. It was withdrawn by NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as *SHA-1*. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. However, NSA did not provide any further explanation or identify the flaw that was corrected. Weaknesses have subsequently been reported in both SHA and SHA-1. SHA-1 appears to provide greater resistance to attacks, supporting the NSA's assertion that the change increased the security.



One iteration within the SHA-1 compression function:
A, B, C, D and E are 32-bit words of the state;
F is a nonlinear function that varies;
n denotes a left bit rotation by *n* places;
n varies for each operation;
Wt is the expanded message word of round t;
Kt is the round constant of round t;
Denotes addition modulo 232

II. Litrature Survey

Desktop sharing commonly refers to a remote frame buffer technology. Desktop sharing allows a user to send screen data to be drawn elsewhere and receive input remotely. Its applications vary from remote system administration to accessing virtual machines. There has been much research concerning the use of desktop sharing as a platform for collaboration. A few useful features appear in several papers.

The BASS Application Sharing System established the idea of applying a secondary protocol to re-encode video and stream it separately from the frame buffer for any video playing on the screen. Additionally the sharing system supports per-application sharing by removing all non-application specific information from the remote frame buffer. In one system researchers enhanced the Virtual Network Computing (VNC) protocol by adding an additional layer of authentication to allow for view-only or normal interactivity connections.

Systems that support multicast (multiple people only seeing one screen) tend to use the Binary Floor Control Protocol to determine controllability of the screen at any one point in time. There are also other papers of interest that cover non-desktop sharing collaboration. For example, research on remote pair programming, where two users work on the same code at the same time using shared cursors and synchronized codebases, differs from desktop sharing because both users are still seeing different desktops. Instead of actually visualizing the other collaborator's desktop, a user of the Sangam tool has a synchronized view and cursor with the other collaborators. This approach works well in very specialized environments such as programming Integrated Development Environments (IDEs) but lacks usability in more general scenarios. Unfortunately no hard research has been done on the efficacy of the technique but it is important to remember that desktop sharing is just one facet of collaboration technology.

Help desk is a generic name typically associated with an end-user support center. Prior to the creation of a dedicated help desk, end-users often resorted to contacting a friend or colleague for assistance. Today's savvy technology managers realize that it is critical to transform outdated "help desks," which rely primarily on telephone communications, into efficiently managed "service desks" that efficiently and economically accommodate multiple forms of interaction - from voice and data to email and instant messaging. They also understand that by transitioning to self-assist and remote incident resolution they can reduce service desk operational costs by half, while dramatically improving the quality of service provided.

Although the telephone is the preferred method of seeking support, end-users can encounter frustration when calling the help desk. End-users often lack confidence that they will be able to adequately describe the issue they are experiencing or fear embarrassment for their lack of application and or computer knowledge and skills. This can lead to confusion and misinterpretation for the support specialist as they attempt to resolve the issue. Concern over a language barrier is a potential drawback of phone support as well. The end-user may become frustrated and abandoned the call before their issue is resolved if they're unable to understand a support specialist due to a thick accent.

In order to overcome such problem, the Help Desk can capture the customers desktop and solve the problem themselves.

III. System Architecture

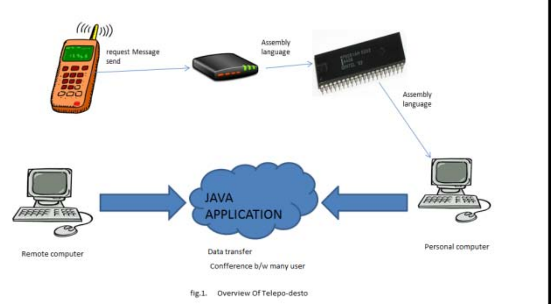


Fig. 1

A user has to send an SMS by the cell phone to the home server. It will be received through hardware modules like modem, microcontroller and a microprocessor. The system responds back by sending an acknowledgment message asking user to prove his /her authenticity.

Incase of authentic password reception, the system generates a onetime password for the user to establish the connectivity. As soon as the system is connected, the data transfer can take place. For providing security to the data transmission, a very powerful encryption algorithm is used.

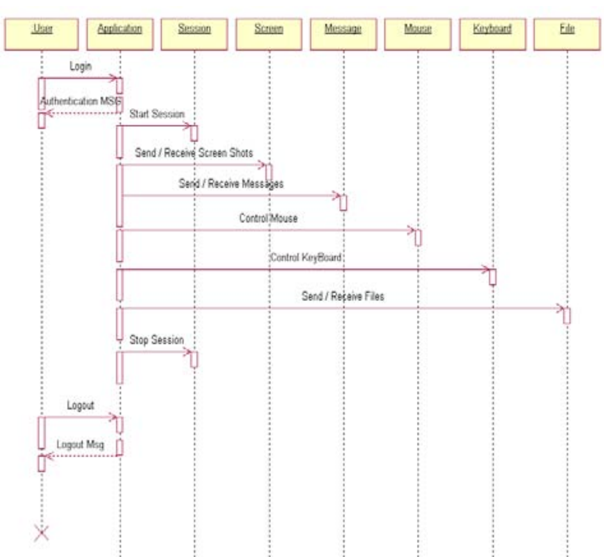


Fig. 2 : Sequence Diagram

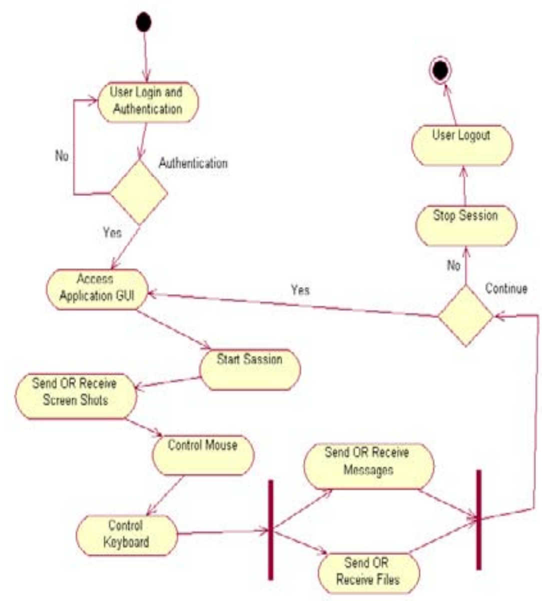


Fig. 3 : Use case diagram

IV. Advantages

1. Anyone can access data from a PC anywhere and anytime by simply sending an SMS.
2. It saves money by lowering your monthly utility bills.
3. Easy to operate and use as Mobile Phones are extensively used.
4. Has negligible portability issues as Cell Phones easily fit in pockets.

V. Disadvantages

1. The energy required to run the devices .This problem can be removed by using solar technology to run the system.
2. Installation will need expertise person the local resident will face a problem in installation.
3. There is maintenance of this system is required as this is a new technology and have potential risks. Regular checkup of the security and other critical operations are necessary for such new technology.

VI. Conclusion

In conclusion, I feel that the proposed system has a great potential in revolutionizing the concept of Desktop Sharing. As Mobile phones are small in size and easily portable, they become a smarter choice for accessing the remote desktop than a PC or a laptop. They can be easily carried and handled by their users. They are a smarter means of working on Remote Systems than a traditional desktop computer or a laptop. Also a cell phone can become a remote control for its users in switching on or off the light bulbs or also act as an indicator showing temperature readings in high temperature zones.

Global Journal of Computer Science and Technology (E) Volume XII Issue XV Version I Year 2012

References Références Referencias

1. Two Factor Authentication Using Mobile Phones Fadi Aloul, Syed Zahidi, Wassim El-Hajj.
2. Towards Ubiquitous Computing via Secure Desktop Service Pan-Lung Tsai, Student Member, IEEE, and Chin-Laung Lei, Member, IEEE.
3. A Herzberg,"Payments and Banking with Mobile Personal Devices", Communications of the ACM,46(5),53-59, May 2008.
4. J. Brainard, A. Juels, R. L. Rivest," Fourth Factor Authentication": ACM CCS, 168-179, 2010.
5. National Institute on Standards and Technology Computer Security Resource Center, NIST's Policy on Hash Functions, March 29, 2009.
6. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering (http:/ / www. schneier. com/ book-ce. html), John Wiley & Sons, 2010.
7. A. Josang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities" in Proc. of the Australian information security workshop conderence on sACSW frontiers, 43-48, 2003.

Global Journals Inc.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 15 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Controlling the Coverage of Wireless Sensors Network Using Coverage in Block Algorithm

By Rashid Azim

ICMS University Campus, Hayyatabad

Abstract - This research investigate the modeling of Blocks, Present in the sensing field and its impact in the computation of coverage path in wireless sensor networks (WSNs). The solutions of these problems are proposed using techniques from Approximation algorithm. In order to accomplish the designated task successfully, sensors need to actuate, compute and disseminate the acquired information amongst them. Intuitively, coverage denotes the quality of sensing of a sensor node. While a sensor senses. It needs to communicate with its neighboring sensor nodes in order to disseminate the acquired data. That is where connectivity comes in to place. In fact, coverage and connectivity together measure the quality of service (QoS) of a sensor network. Coverage and connectivity in wireless sensor networks are not unrelated problems. Therefore, the goal of an optimal sensor deployment strategy is to have a globally connected network, while optimizing coverage at the same time. By optimizing coverage, the deployment strategy would guarantee that optimum area in the sensing field is covered by sensor, as required by the underlying application, whereas by ensuring that the network is connected, it is ensured that the sensed information is transmitted to other nodes and possibly to a centralized base station (called sink) which makes valuable decision for the application. Many recent and ongoing research in sensor networks focus on optimizing coverage and connectivity by optimizing node placement strategy, minimizing number of nodes to guarantee required degree of coverage, maximizing network lifetime by minimizing energy usage, computing the most and least sensed path in the given region and so on. To solve these optimizing problems related to coverage, exiting research uses mostly probabilistic technique based on random graph theory, randomized algorithm, computational geometry, and so on. Of particular interest to us is the problem of computing the coverage in block (CIB), where given a set of homogeneous sensors deployed in a field and the initial location of an agent that needs to move through the field, determine the path that is most protected by the sensors.

GJCST-E Classification : *C.2.1*

CONTROLLING THE COVERAGE OF WIRELESS SENSORS NETWORK USING COVERAGE IN BLOCK ALGORITHM

Strictly as per the compliance and regulations of:

OPEN ASSOCIATION OF RESEARCH SOCIETY, USA
RESEARCH | DIVERSITY | ETHICS

Controlling the Coverage of Wireless Sensors Network Using Coverage in Block Algorithm

Rashid Azim

Abstract - This research investigate the modeling of Blocks, Present in the sensing field and its impact in the computation of coverage path in wireless sensor networks (WSNs). The solutions of these problems are proposed using techniques from Approximation algorithm. In order to accomplish the designated task successfully, sensors need to actuate, compute and disseminate the acquired information amongst them. Intuitively, coverage denotes the quality of sensing of a sensor node. While a sensor senses. It needs to communicate with its neighboring sensor nodes in order to disseminate the acquired data. That is where connectivity comes in to place. In fact, coverage and connectivity together measure the quality of service (QoS) of a sensor network. Coverage and connectivity in wireless sensor networks are not unrelated problems. Therefore, the goal of an optimal sensor deployment strategy is to have a globally connected network, while optimizing coverage at the same time. By optimizing coverage, the deployment strategy would guarantee that optimum area in the sensing field is covered by sensor, as required by the underlying application, whereas by ensuring that the network is connected, it is ensured that the sensed information is transmitted to other nodes and possibly to a centralized base station (called sink) which makes valuable decision for the application. Many recent and ongoing research in sensor networks focus on optimizing coverage and connectivity by optimizing node placement strategy, minimizing number of nodes to guarantee required degree of coverage, maximizing network lifetime by minimizing energy usage, computing the most and least sensed path in the given region and so on. To solve these optimizing problems related to coverage, exiting research uses mostly probabilistic technique based on random graph theory, randomized algorithm, computational geometry, and so on. Of particular interest to us is the problem of computing the coverage in block (CIB), where given a set of homogeneous sensors deployed in a field and the initial location of an agent that needs to move through the field, determine the path that is most protected by the sensors.

I. Introduction

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path any single device are minimal, the composition of offers radical new technological possibilities.

The power of wireless sensor networks lies in there ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices computing environments, to in situ monitoring of the health of structures or equipment.

While often referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world.

The most straight forward application of wireless sensor network technology is to plant could be easily monitored for leas by hundreds of sensors that automatically form a wireless interconnection network and immediately report the detection of any chemical leaks.

Unlike traditional wired system, deployment costs would be minimal. Instead of having to deploy thousands of feet of wire routed through protective conduit, installers simply have to place quarter-sized device, such as the one pictured in Figure 1-1, at each sensing point. The network could be incrementally extended by simply adding more devices-no rework or complex configuration. With the devices presented in this research, the system would be capable of monitoring for anomalies for several years on a single set of batteries.

In addition to drastically reducing the installation costs, wireless sensor networks have the ability to dynamically adapt to changing environments, adaptation mechanisms can respond to changes in network topologies or can cause the network to shift between drastically different modes of operation. For example, the same embedded network performing leak monitoring in a chemical factory might be reconfigured into a network designed to localize the source of a leak and track the diffusion of poisonous gases. The network could then direct workers to the safest path for emergency evacuation.

II. Wireless Coverage Problems

Coverage is the measure of QoS of sensing function and is subject to a wide range of interpretations due to large variety of sensors and applications. Considering the coverage concept, different problems can be formulated, based on the subject to be covered (Area versus discrete points) and on the design choices, such as sensor development method, additional critical

Author : ICMS, Hayatabad, Peshawar, Pakistan.
E-mail : rashidazim@yahoo.com

requirements, sensing and communication radius N. Xu et al. (2004).

A wide classification can be done with respect to the type of algorithm used as well. Centralized versus distributed/localized. We also compare these approaches and algorithm based on their goals, assumption, complexities and usefulness in practical scenarios. Objective of these design choices are either to maximize network lifetime; minimize number of sensors or optimize degree of coverage, and so on a a comprehensive study on coverage connectivity research can be found in Akyidiz et al. (2002).

Coverage can be classified of three types based on the subject to be covered. Area coverage, point coverage and barrier coverage. The most studied problem is the area research is going on in both the static and mobile sensor network D. Tian et al. (2002).

The design choices are given bellow:

1. Sensor deployment strategies: deterministic versus random. A deterministic sensor placement may be feasible in friendly and accessible environments. Random sensor distribution is generally considered in military applications and for remote or inhospitable areas.
2. Energy Requirement: In the most typical scenarios, energy requirement is a big factor as sensors are usually limited with respect to its battery life. Several research work has been done on energy efficient coverage.
3. Sensing and communication Radii: Homogeneous/ Heterogeneous sensor network is the subject of interest here. While constraints are less in homogeneous sensor network heterogeneous sensor network has a wider scope in applications.

A broader classification of coverage problems can also be done in terms of their goals, assumptions, algorithm complexities and practical applicability. The three categories are

1. Coverage based on the exposure path
2. Coverage based on sensor deployment strategies
3. Miscellaneous strategies

III. Minimal Exposure Path: Worst Case Coverage

Coverage is a measure of how well a sensing field is covered with sensors.

Informally stated, it can be defined as the expected average ability of observing a target moving in the sensing field. The minimal exposure path provides valuable information about the worst case coverage in sensor networks.

The basis of the proof adopted to compute the exposure path of one sensor lies in the fact that since any point on the dotted curve is closer to the sensor than any point lying on the straight line segment along the edge of the square; the exposure is more in the former case.

Also, since the length of the dotted curve is longer than the line segment, the dotted curve would induce more exposure with an object travels along it, given that the time duration is the same in both the cases. Furthermore, this method is extended when the sensing region is a convex polygon and the sensor is located at the center of that inscribed circle.

This intuition can further be extended to compute the minimal exposure path under the scenario of many sensors. To simplify, the problem can be transformed from the continuous domain into a tractable discrete domain by using an m ₤ n grid. The minimal exposure path is then restricted to straight line segment connecting any two consecutive vertices of a grid square. This approach transforms the grid into an edge weighted graph and computes minimal exposure path using Dijkstras single source shortest path algorithm.

IV. Maximal Exposure Path: Best Case Coverage

A maximal exposure path between two arbitrary points's and t in a sensing field is a path following which the total exposure is maximum. It can be interpreted as a path having the best case coverage. It has been proved by Z. Butler (2004. That finding the maximal exposure path is NP-hard because it is equivalent to finding the longest path in an undirected weighted graph, which is known to be NP-hard. However, there exist several heuristics to achieve near-optimal solutions under the constraints that objects speed, path length, exposure value and times.

V. Maximal Breach Path: Worst Case Coverage

A minimal exposure path is equivalent of finding a worst case coverage path, which provides valuable information about node deployment density in the sensing field. A very similar concept to find out worst case coverage path is the notation of maximal path Meriall (2003).

A maximal breach path through a sensing field starting at s and ending at t is a path, such that for any point p on the path, the distance from p to the closest sensor is maximum. The concept of Voronoi diagram, a well known construct from computational geometry is used to find a maximal breach path in a sensing field.

It is also proved intuitively since by construction, the line segments in a Voronoi diagram maximizes the distance from the closest sites, the maximal breach path must lie along the Voronoi edges. The algorithm then checks the existence of a path from s to t using breadth-first-search (BFS) and uses binary search between the smallest and largest weight in the computed Voronoi graph to find the maximal breach path.

VI. Maximal Support Path: Best Case Coverage

A maximal Support path through a sensing field starting at s and ending at t is a path, such that for any point p on the path, the distance from p to the closest sensor is minimized. This is similar to the concept of maximal exposure path. However, the difference lies in the fact that a maximal support path algorithm finds at any given time instant.

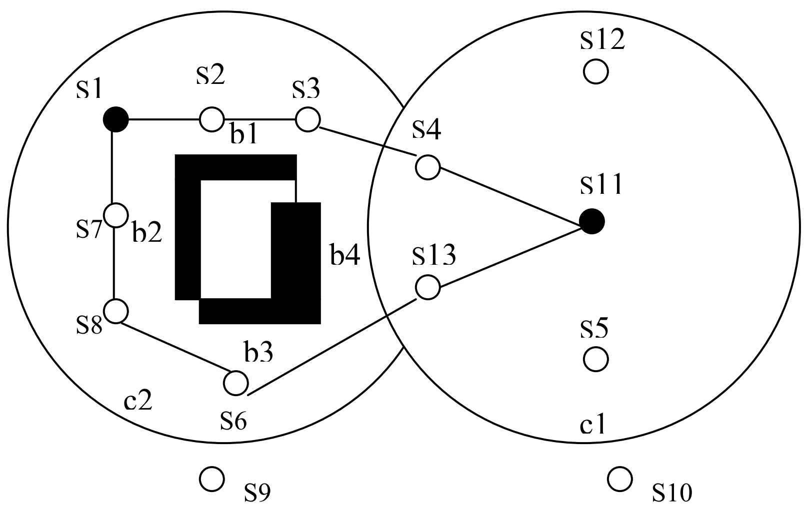
Such that the exposure on the path is no less than some particular value which should be maximized. A maximal support path in a sensing field can be found by replacing the Voronoi diagram by its dual, Delaunay triangulation where the edges of the underlying graph are assigned weights equal to the length of the corresponding line segments in the delaunay triangulation Z. Butler (2004). This ends our brief discussion on coverage problems based on exposure path in WSNs. Next, we discuss different deployment strategies which impact coverage in WSNs.

VII. Coverage Based on Sensor Deployment Strategies

The second approach to the coverage problem is to find sensor deployment strategies that would maximize the coverage as well as maintain a globally connected network graph. Several deployment strategies have been studied for achieving an optimal sensor network architecture that would minimize cost, provide high sensing coverage, and be resilient to random node failure etc. the most usual deployment strategy of sensor nodes are random deployment.

However, random placement does not guarantee full coverage because it is stochastic I nature, hence often resulting in accumulation of nodes at certain areas in the sensing field whereas leaving other areas deprived of nodes. Keeping this in mind, some of the deployment algorithms try to find new optimal sensor locations after an initial random placement and moves the sensors to those locations, achieving maximum coverage. These algorithms are applicable to only mobile sensor networks.

Research has also been conducted in mixed sensor networks, where some of the nodes are mobile and some are static; and approaches are proposed to detect coverage holes after an initial deployment and trying to heal or eliminate those holes by moving sensors. It should be noted that an optimal deployment strategy should result not only in a configuration that would provide sufficient coverage, but also satisfy certain constraints such as node connectivity and network connectivity [40].



Sensor Field with Four blocks b1, b2,..., b4 and sensors

VIII. Algorithm: Find Best Coverage(S:s:T)

1. Find closest sensor node of the starting point s if itself is not a sensor node. Assume S7 is the closest sensor node. Similarly, find the closest sensor node S13 of the ending t.
2. Each sensor node S locally constructs all edges Sv of the relative neighborhood graph broadcasts its location information and listen to the broadcasting by its neighbors. Thus, after this step, we assume that each node S has the location information of NI(S).
3. Assign each constructed edge Sv with weight 1.
4. Run a distributed shortest path algorithm to compute the shortest path Connecting Ss and St. Here, the weight of a path is the maximum weight of all of its edges.

Here a path is the shortest path if it has the minimum weight among all paths connecting Ss and St. the Bellman-Ford algorithm M. Bauer (2004) can be modified to solve this shortest path problem.

IX. Conclusion

In this thesis we present an overview of coverage and the coverage related problems in the presence of block. We also present an algorithm to overcome this problem by using approximation algorithm called CIB coverage in block algorithm. The upcoming technological advances will most likely be applied to decreasing the power consumption of the device. In trun, this will enable a reduction of physical size of the energy storage required for any given application. as for tighter levels of integration, the cost/size point represented by the spec platform has reached the point of diminishing returns. Further reduction in the physical size of the radio, processing, and storage is no longer necessary. Only a select few application have the need for a device that is smaller that 2.5 mm × 2.5 mm. However, all application scenarios can benefit from reduced power consumption which is translated into longer network lifetime and / or increased sample rate.

References Références Referencias

1. Akyidiz, W. Su, Y. sankarasubramaniam, and E. Cayirci. "Wireless sensor networks: A survey, " Computer Network(Elsevier) Journal, vol. 38, no. 4, pp. 393-422, Mar, 2002.
2. A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Application Driver for wireless communications Technology". Workshop on Data Communications in Latin America and Caribbean, San Jose, Costa Rica, April 2001.
3. Berkely, University of California, 800 nodes, "self-organized wireless sensor Network", 2001: http://today.cs.berkeley.edu/800demo/.
4. D. Tian and N. D. Georganas, "A coverage preserving node scheduling scheme for large wireless sensor networks". Proc. of the 1st ACM workshop on wireless sensor networks and applications, 2002
5. H. Baldus, K. Klabunde, and G. Muesch," Reliable Set-Up of Medical Body Sensor Networks". Proc. EWSN 2004, Berlin, Germany, January 2004.
6. M. Bauer, L. Jendoubi, and O. Siemoneit, "Smart Factory Mobile Computing in Production Environments". WAMES 2004, Boston, USA, June 2004.
7. N. Xu, S. Rangwala, K.K. Chintalapudi, D.Ganesan, A. Broad, R. Govindan, and D. Estrin, "A Wireless Sensor Network for Structural Monitoring". Sensys 2004, Baltimore, USA, November 2004.
8. W. M. Meriall, F. Newberg, K. Sohrabi, W. Kaiser, and G. Pottie, "Collaborative Networking Requirements for Unattended Ground Sensor System". Proc. IEEE Aerospace Conference, March 2003.
9. Z. Butler, P. Corke, R. Peterson, and D. Rus, "Networked Cows: Virtual Fences for Controlling Cows". WAMES 2004, Boston, USA, June 2004.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 15 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

ESAHR: Energy Efficient Swarm Adaptive Hybrid Routing Topology for Mobile Ad hoc Networks

By B. M. G. Prasad & Dr. P.V.S. Srinivas

CMJ University, Schillong, Meghalaya (state), India

Abstract - Ad hoc networks consist of independent self structured nodes. Nodes use a wireless medium for exchange their message or data, therefore two nodes can converse directly if and only if they are within each other's broadcast range. Swarm intelligence submits to complex behaviors that occur from very effortless individual activities and exchanges, which is frequently experienced in nature, especially amongst social insects such as ants. Although each individual (an ant) has little intelligence and simply follows basic rules using local information gained from the surroundings, for instance ant's pheromone track arranging and following activities, globally optimized activities, such as discovering a shortest route, appear when they work together as a group. In this regard in our earlier work we proposed a biologically inspired metaphor based routing in mobile ad hoc networks that referred as Swarm Adaptive Hybrid Routing (SAHR). . With the motivation gained from SAHR, here in this paper we propose a energy efficient swarm adaptive hybrid routing topology (ESAHR). The goal is to improve transmission performance along with energy conservation that used for packet transmission In this paper we use our earlier proposed algorithm that inspired from Swarm Intelligence to obtain these characteristics. In an extensive set of simulation tests, we evaluate our routing algorithm with state-of-the-art algorithm, and demonstrate that it gets better performance over a wide range of diverse scenarios and for a number of different assessment measures. In particular, we show that it scales better in energy conservation with the number of nodes in the network.

Keywords : Manet, Swarm intelligence, hybrid routing, unicast routing, ACO.

GJCST-E Classification : B.4.3

ESAHR ENERGY EFFICIENT SWARM ADAPTIVE HYBRID ROUTING TOPOLOGY FOR MOBILE AD HOC NETWORKS

Strictly as per the compliance and regulations of:

ESAHR: Energy Efficient Swarm Adaptive Hybrid Routing Topology for Mobile Ad hoc Networks

B. M. G. Prasad [α] & Dr. P.V.S. Srinivas [σ]

Abstract - Ad hoc networks consist of independent self structured nodes. Nodes use a wireless medium for exchange their message or data, therefore two nodes can converse directly if and only if they are within each other's broadcast range. Swarm intelligence submits to complex behaviors that occur from very effortless individual activities and exchanges, which is frequently experienced in nature, especially amongst social insects such as ants. Although each individual (an ant) has little intelligence and simply follows basic rules using local information gained from the surroundings, for instance ant's pheromone track arranging and following activities, globally optimized activities, such as discovering a shortest route, appear when they work together as a group. In this regard in our earlier work we proposed a biologically inspired metaphor based routing in mobile ad hoc networks that referred as Swarm Adaptive Hybrid Routing (SAHR). . With the motivation gained from SAHR, here in this paper we propose a energy efficient swarm adaptive hybrid routing topology (ESAHR). The goal is to improve transmission performance along with energy conservation that used for packet transmission In this paper we use our earlier proposed algorithm that inspired from Swarm Intelligence to obtain these characteristics. In an extensive set of simulation tests, we evaluate our routing algorithm with state-of-the-art algorithm, and demonstrate that it gets better performance over a wide range of diverse scenarios and for a number of different assessment measures. In particular, we show that it scales better in energy conservation with the number of nodes in the network.

Keywords : Manet, Swarm intelligence, hybrid routing, unicast routing, ACO.

I. Introduction

In disparity to merely establishing accurate and efficient routes among pair of nodes, one significant goal of a routing topology is to remain the network functioning as long as potential. This objective can be consummate by reducing mobile nodes energy not only through active communication but also when they are not participating. Communication energy control and load allocation are two approaches to reduce the energy levels of active communication, and sleep/energy-down mode is used to reduce energy through inactivity.

Author α : Associate Professor & Head, Department of Information Technology, Brindavan Institute of Technology and Science, Kurnool, Andhrapradesh, India. Pursuing his Ph.D in computer science and engineering under the guidance of Dr.P.V.S.Srinivas at CMJ UNiversity, Schillong, Meghalaya (state), India.
E-mail : bmgprasad@gmail.com
Author σ : Professor & Head, Department of Computer Science & Engineering Geethanjali College of Engineering & Technology, Keesara, Hyderabad, Andhrapradesh, India.
E-mail : pvssrinivas_70@yahoo.com

Wireless ad hoc networks typically consist of mobile battery functioned computing devices that correspond over the wireless medium. While the dispensation ability and the memory space of computing devices augment at a very rapid speed, the battery method wraps distant behind. Therefore, it is significant to obtain energy preservation schemes to augment the device and network process time.

In wireless networks, the broadcasted signal is assuaged at the speed of $1/d^n$, where d is the distance among sender and receiver and n is the route loss exponent with approximate value between 2 and 6 depending on the equipped environment. As an alternative of using the maximum energy for transmissions all the time, with energy control, a sender can regulate the communication energy according to d. Though, link level energy control cannot make sure that the end-to-end energy utilization from a source to a destination is minimal. To conserve energy, many energy efficient routing topologies have been projected [1, 2, 3, 4, 5, 6, 7, 8, 9]. These topologies can be usually classified into two categories: Minimal Energy usage routing topologies [1, 2, 3, 4, 5, 6] and Utmost Network Lifespan routing topologies [8, 9].

In existing minimal energy routing topologies, signaling packets are often transmitted at the maximum energy to reduce the hidden terminal problem as a result of using asymmetric transmission energy from different adjacent nodes. The signaling packet effects by more collisions, for instance the RTS packet in 802.11, would use noteworthy amount of energy. Without taking into consideration the energy utilized for transmitting, the route exposed could utilize much more energy than a route selected based on a more precise energy utilization model. In addition, the majority of literature works paying attention only on the direction of new hop level transmission cost metric. Once a new hop level transmission cost is resultant, the traditional shortest route routing topologies, for instance AODV (Ad hoc On Demand Distance Vector) and DSR (Dynamic Source Routing) topologies, are customized to search for the minimum cost route. Though, such straightforward customization would lead to numerous problematic issues. Foremost, the routing overhead in route detection phase is excessive, which not only utilizes a significant amount of energy but also shows the way to a long route establishment delay impediment. Second, the route maintenance plan used in conservative

Global Journal of Computer Science and Technology (E) Volume XII Issue XV Version I Year 2012

shortest route topology is not suitable for maintaining energy efficient route in a mobile environment.

In this paper, we first present a comprehensive argument on the problems in conventional energy efficient routing topologies. We then derive a new hop level transmission cost model to account for energy utilization due to signaling packets at MAC layer, and make available the schemes for approximation the parameters necessary for calculating the hop level transmission cost. Based on the new energy utilization model, we extend our earlier work Swarm Adaptive Hybrid Routing topology [14] as Energy Efficient Swarm Adaptive Hybrid Routing topology for energy conserved data transmission along the route discovered by swarm adaptive hybrid routing topology [14].

This paper discussing the related work in section II that followed by the exploration of the proposed energy efficient swarm adaptive hybrid routing topology in section III. Section IV elaborates the considered basic routing topology SAHR and section V explores simulations and results analysis, which followed by the conclusion of the proposal and experiments.

II. Related Work

There are numerous obtainable routing topologies for wireless ad hoc networks. In general, these topologies can be categorized as proactive, on-demand, and hybrid. In proactive routing topologies, all nodes need to advertise the routing information periodically to keep an up to date view of the network topology. Different from table driven routing topologies, on-demand routing topologies create a transmission route only when required by the source node. Hybrid topologies combine both approaches. For example, in Zone level Routing Topology (ZRP), proactive routing scheme is used for intra-zone level routing and on-demand routing scheme is used for inter-zone level routing. Most of energy efficient schemes proposed in the literature modified on-demand routing topologies such as AODV [16] or DSR [17] to build energy efficient route since the routing overhead is very high in proactive routing topologies [2]. In on-demand routing topologies such as AODV, a node will initiate a route detection process if it needs to find a route to a target node. It transmits the route request packet and waits for the reply from the target node.

The adjacent nodes that receive these route request packet will retransmit it, and so on. To decrease the routing overhead, the intermediary nodes will only retransmit the first conventional route request packet and discard the subsequent duplicate ones. In addition, the target node only replies to the first route request packet. It is obvious that the overhead for these on demand routing topologies is $O(n)$, where 'n' is the number of nodes belongs to the network considered. Route detection in energy efficient routing topologies is however fairly dissimilar. The intermediary nodes could not simply discard the duplicate route request packets now as such packets may come from more energy efficient routes. That is, the intermediate nodes need to process and retransmit the duplicate route request packets if they come from a more energy efficient route. Consequently, the nodes may require transmitting the same route request packet numerous times.

In the context of the routing topology SAHR [14], several successful routing algorithms have been proposed taking inspiration from ant colony behavior and the related framework of Ant Colony Optimization (ACO) [8A]. Examples of ACO routing algorithms are AntNet [6A] and ABC [13].

The ACO routing algorithms mentioned before were developed for wired networks. They work in a dispersed and restricted way, and are capable to study and adjust to transformations in traffic models. However, changes in MANETs are much more drastic: in addition to disparities in traffic, both topology and number of nodes can change incessantly. Additional complexities are caused by the partial realistic bandwidth of the communal wireless channel, even though the data transmission pace of wireless communication can be fairly high, algorithms in use for MAC, such as IEEE 802.11 DCF [15], create a lot of overhead both in terms of control packets and delay, lessening the effectively available bandwidth. The autonomic control confronts are consequently much bigger, and new designs are essential to assurance even the basic network functions.

III. Energy Efficient Swarm Adaptive Hybrid Routing Topology for Mobile Ad Hoc Networks

1. When a route to a target node D is obligatory, but not known at source node S, S transmits a Rout Trace Swarm Agent RTSA to discover a route to D.
2. When D receives the RTSA from S, it initiates to transmit RTSA as Route Confirmation Swarm Agent RCSA, which transmits in backward manner through the route that traced by parent RTSA. The RCSA updates the routing table and emission table of all the nodes in the route from S to D, allowing for data transfer from S to D. Here emission table is maintained by each node n to store emission attribute value sav_{ni} of its each forwarding neighbor ni. The emission attribute value is similar to pheromone repository of the biological swarm agent.
3. When a route fall shorts at an intermediate node X then SAHR reinitiates route detection process.

4. When a route at D is known to S, SAHR deterministically chooses the route by opting to best forwarding hop level neighbor ni based on their hop level delay and number of hops to reach the destination.

IV. Swarm Adaptive Hybrid Routing Topology [14]

SAHR's style is stimulated by Swarm Agent Optimized routing algorithms for wired networks. It uses swarm agents that follow and update emission tables in an indirect agent interaction for the modification of the surroundings learning method. Knowledge packets are routed stochastically consistent with the learned tables. A vital distinction with alternative Swarm Agent Optimized routing algorithms is that SAHR could be a hybrid algorithm, so as to deal higher with the precise challenges of Manet environments. It's reactive within the sense that nodes solely gather routing info for destinations that they're currently communicating with, whereas it's proactive as a result of nodes try and maintain and improve routing info as long as communication goes on. we tend to build a distinction between the trail setup, that is that the reactive mechanism to get initial routing info a couple of destination at the beginning of a session, and route maintenance and improvement, that is that the traditional mode of operation throughout the course of a session to proactively adapt to network changes. The routing info obtained via indirect agent interaction is unfolded between the nodes of the Manet in hop level neighbor info exchange method to supply secondary steerage for the swarm agents. Within the following we offer a broaden description of the SAHR.

SAHR's design is inspired by swarm agent optimized routing algorithms for wired networks. It uses swarm agents which follow and update emission tables in an indirect agent interaction about the modification of the environment learning process. Data packets are routed orderly in accord to the learned tables. An important difference with other Swarm Agent Optimized routing algorithms is that SAHR is a hybrid algorithm, in the process of dealing better with the specific MANET confronts. It is on-demand in the sense that nodes only collect routing information for targets which they are at present corresponding with, while it is proactive because nodes try to maintain and improve routing information as long as communication is going on. We make a distinction between the route setup, which is the on demand mechanism to acquire initial routing information about a destination at the start of a session, and route maintenance and perfection, which is the usual mode of process through the course of a session to proactively acclimatize to network changes. The routing information obtained via indirect agent interaction learning is spread between the nodes of the MANET in a hop level neighbor information exchange process to provide secondary guidance for the swarm agents. In the following we provide a concise description of each of these components.

a) Pheromone Indicator for ESAHR

Routes are implicitly outlined by the emission tables that are kept regionally at every node. An entry g_{ni} of the emission table ST_i at node i that consider as pheromone indicates about the goodness of the routing from node i to via immediate node ni contains a price indicating the estimated goodness of going from i over neighbor ni to reach destination d. This goodness is derived from the combination of route end-to-end delay and range of hops. These are commonly used quality measures in Manets. Combining the number of hops with end-to-end delay between immediate node ni to current node i and destination node d is a way to swish out presumably giant oscillations within the time estimates gathered by the swarm agents. Since SAHR solely maintains info regarding destinations that are active during a communication session, and due to continuous change at neighbor nodes, the filling of the emission tables is dynamic.

b) Route Detection in ESAHR

The source node s determines the route to node d via transmitting Route Trace Swarm Agent $RTSA$. At each neighbor hop that received $RTSA$, transmits the same to their neighbor hops. This process is recursive for each $RTSA$ till it received by destination node d. Upon receiving the $RTSA$, the destination node d initiates to transmit Routing-route Confirmation Swarm Agent $RCSA$ that derived from $RTSA$. $RCSA$ Transmits in backward manner through the route that traced by parent $RTSA$. Upon reaching each node i in the routing route, $RCSA$ updates pheromone indicator value g_{ni} of relay hop node ni of the current node i in the routing route opted by $RCSA$. The process of updating the pheromone indicator value is as follows: During the transmission of swarm-agent $RCSA$, it collects the time $t_{ni \to i}$ taken to reach each node i from relay hop node ni the '$RCSA$'is coming from. The estimated time $t_{i \to d}$ to transmit a data packet from node i to destination node d via $\{ni, ni+1, ni+2 ... ni+n\}$ is measured using equation (1).

$$t_{i \to d}^{ni} = t_{(ni+n) \to d} + \sum_{k=n}^{1} t_{(ni+k-1) \to (ni+k)} \quad (1)$$

And then pheromone indicator value will be measured using equation (2) and (3) that fallows

Global Journal of Computer Science and Technology (E) Volume XII Issue XV Version I Year 2012

$$\left(t_{i\to d}^{ni}\right)' = \left[t_{i\to d}^{ni}\right]^{-1} * 100 \quad (2)$$

$$g_{ni} = \frac{\left(t_{i\to d}^{ni}\right)'}{hc_{i\to d}^{ni}} \quad (3)$$

Here in equation (3), $hc_{i\to d}^{ni}$ indicates the hop count in route from current node i to destination node d via relay hop node ni.

The inverse value of the estimated time $t_{i\to d}^{ni}$ for a data packet to travel from node i to destination node d indicates the optimality of the route between nodes i to destination node d via relay node ni. Hence the equation (2) is significant.

Upon receiving swarm agent $RCSA$, the source node s also updates its emission table with pheromone indicator value g_{ni} of each neighbor hop ni the $RCSA$ coming from.

c) Energy efficient Data transmission and route maintenance in ESAHR

The routing-route maintenance will be carried out in proactive manner and will be initiated at destination node d. The data transmission and route maintenance strategies explored in fallowing subsections.

i. *Data Transmission with minimal Energy Usage*

In the process of transmitting data, source and hop level node selects the target neighbor relay hop dynamically. Initially source node finds best neighbor ni based on pheromone indicator value of the nodes registered in its emission table. Opting to a neighbor relay hop ni with best pheromone indicator value g_{ni}, transmits data packet to selected neighbor relay hop ni .Upon receiving the data packet the neighbor relay hop registers the sender's information in routing cache. The strategy of selecting neighbor relay hop dynamically and transmitting data packet is recursive at each neighbor hop relay node. This process will be halted once the data packet received the destination node d. And as an extension to this process a energy conservation mechanism introduced to minimize the energy usage in data transmission that described in section ii that follows.

ii. *Minimal Energy Usage for data transmission in ESAHR*

The nodes are having limited energy and storage capacity, Hence the Energy efficient Swarm Adaptive Hybrid Routing topology has been proposed that saves energy resources. Here in this proposed ESAHR model the RTS packet takes the energy used for communication by the source node of that RTS. Then the target node of that RTS finds the state of the signal that used to send out RTS.

$$SS_r = SS_s(\alpha / 4\pi d)^2 S_T S_R$$

Here α is the wavelength of the signal to be carried, d is the distance travelled by RTS between source and target nodes. ST is the single plane uniform radio wave transmission threshold of source node antennas and SR is the single plane uniform radio wave receiving threshold of target node antennas. 'SS_s' is the actual state of the transmission signal energy at the source node s. And SS_r is the state of the signal energy that found at target node r, which used to transmit RTS.

Then the loss state of signal SS_l during routing can be found at target node r by using the following equation.

$$SS_l = SS_r - SS_s$$

And then this SS_l can be used to find minimal signal state SS_m required at the source node, the equation is as follows

$$SS_m = mh \times (SS_l + RSS_m)$$

Here in the above equation

The 'SS_m' indicates minimal signal state required at the source node s

The 'mh' is the marginal hike threshold that is used to normalize SS_m to handle the inference issues on the target node side.

The 'RSS_m' indicates the minimal signal state required at receiving node side to detect the appropriate signal.

There are a set of topologies available for energy control in mobile ad-hoc networks based on the common energy approach [10]. These topologies are complex and have been analyzed that the variable range transmission energy is a better approach than the general energy.

The proposed ESAHR is capable to conserve the energy even to transmit RTS/CTS packets, which is based on the received signal condition. When a source node needs to transmit data, it initiates the optimal routing strategy such as AODV and then transmits the $RREQ$ packet to the hop level nodes and the $RREP$ packet is received from the intermediate nodes via the shortest route and then enters it in their routing table about the next hop to which the anon data packets are desired to be advanced.

For energy preservation, the RREP packet is recognized by an identifier (id) at the MAC layer and its signal state information is attained from the physical layer. Upon receiving the $RREP$ packet by a node 'r' from a node 's', the node 'r' computes loss state of the signal SS_l during the RREP transmission from node 's' to 'r' and minimal signal state SS_m required at node 's'. And then node 'r' stores minimal signal state required for the node 's' in its routing table.

The process of energy conservation during data transmission in proposed ESAHR as follows:

The source node 's', while sending RTS to its next hop level node r of the routing route, also sends the $SS_m(r)$ stored in its routing table. Here $SS_m(r)$ is the minimal signal state required for r, which is measured and stored in the routing table of node s during route detection. The source node s also includes $SS_m(s)$ as an extra field in the RTS packet. Upon receiving the RTS, the target node r tunes its transmission energy and replies back with 'CTS' packet. Upon receiving the CTS the source node s sends the data with the requisite transmission energy informed by the target node r through 'CTS'.

iii. *Routing Route maintenance*

Upon receiving a packet dp_i, the destination node d verifies the time $t(dp_i)$ taken by dp_i to travel from source node s to destination node d and then measures the end to end delay for data packet dp_i. If end to end delay of dp_i is exceeding the delay threshold τ then it initiates a swarm agent $RCSA$ and transmits towards source node that opts to the route accessed by data packet dp_i. Hence the '$RCSA$' performs the process of updating pheromone indicator value g_{ni} at each hop level relay node in the route. This process explored in equations (1), (2) and (3).

iv. *Handling link failures*

The destination node d initiates swarm agents $RCSA$ to each neighbor relay hop nodes in fixed time intervals. Hence the pheromone indicator values in emission table of each node will be updated in fixed time interval ς.

The pheromone indicator value of any neighbor relay hop ni in emission table of any node i is not valid if time since last update of g_{ni} is greater than time interval ς. This indicates the link failure between node i and destination node d.

V. Experimental Results

We have simulated ESAHR, SAHR, as well as basic AODV topologies in NS2. The position per hop transmission distance is 250m. For energy maintenance function, many smaller hop level nodes are taken. Energy management is used in all three topologies, including normal AODV topology, in which a transmitter adjusts the transmission energy based on its actual distance to the next hop level receiver. The network area in the simulation is fixed to 1200(m) X 1200(m) and the nodes are arbitrarily dispersed in the network. The available transmission energy levels are $1; 5; 10; 15; 20; 25; 30; 35$mW. The Pm is set to 35mW. The session arrival rate follows Poisson distribution and the session interval follows Exponential allocation. The application topology is CBR (Constant Bit Rate) and the source and target pairs are arbitrarily selected. The mobility follows customized random waypoint model [18] with pause time of thirty seconds. For each CBR session, 50 packets are sent for each second. The rate of route loss and collision are projected using method described in [12]. The detection rate, which can be described as filter memory [11], is fixed to nearly 1. A simulation result was gained by averaging over 25 executions with dissimilar seeds.

We consider that there is no energy saving approach for the nodes, and therefore, a node will use energy in monitoring the channel even if it doesn't receive a packet. A node also utilizes energy when overhearing packet transmissions. Therefore, the receiving energy cannot be dynamically controlled. In the simulations, we thus disregard the receiving energy and focus only on the comparison of transmission energy. We first evaluate the accuracy of the proposed cost model, we then study the performance of route detection for each topology, and finally we consider energy utilization as well as RTS retransmissions in both static and mobile environment.

We compared the energy utilization and the average number of RTS retransmissions of the ESAHR, SAHR and basic AODV topologies by varying the following parameters: node count, average size of the data transmission packets, and advent ratio of the connection. The simulation time for each topology is 5 hours. We monitored the total energy utilization of all the packets delivered at target node, the count of delivered packets at target nodes, and the count of retransmissions RTS required for each execution of the simulation. The couple of evaluation metrics that used to evaluate the topologies are:

Energy Utilization per Packet: It is defined by the total energy utilization divided by the total number of packets delivered. This metric indicates the energy efficiency for each topology.

Average RTS Retransmissions required for each Data Packet: It is defined by the total number of RTS retransmissions divided by the total number of packets delivered. The RTS packet is transmitted at the utmost energy usage level and the packet size is very little. The majority of RTS retransmissions are due to collisions, together with the collisions of both RTS messages and data packets. Hence, this metric can indicate the pace of the collision for each topology. Higher collision rate will cause more energy utilization, higher end-to-end delay, and lower throughput.

The simulation results are shown in Fig. 1 and 2. According to these results, ESAHR topology performs the best in terms of Energy Utilization per Packet as well as Average RTS Retransmission per Data Packet, followed by SAHR topology and AODV.

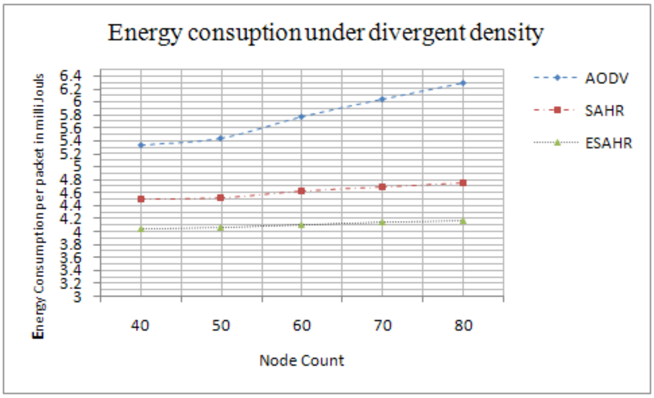


Fig. 1 : Energy Utilization ratio between ESAHR, SAHR and AODV

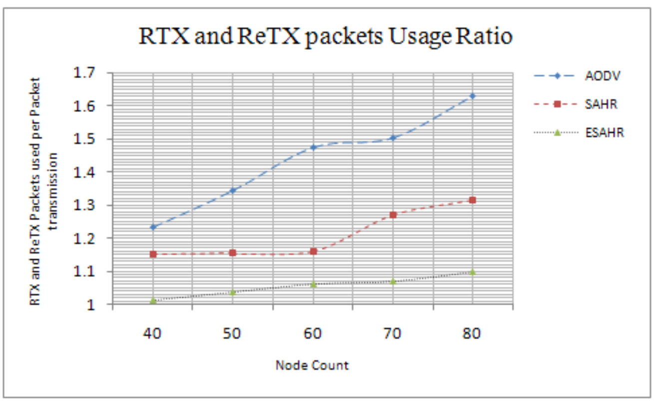


Fig. 2 : RTX and ReTX packets usage Ratio comparison between AODV, SAHR and ESAHR

VI. Conclusion

In this paper we have described ESAHR that is an extension to our earlier routing topology SAHR[14], an Energy efficient Swarm Adaptive hybrid routing (ESAHR) topology for MANETs. The algorithm combines reactive and proactive behavior with swarm intelligence adaptation to deal with the routing challenges of MANETs in an efficient way. This also concern about energy conservation during packet transmission. An efficient hop level transmission cost model to more accurately track the energy utilization due to various factors was explored for packet transmission through the route discovered and maintained under SAHR topology. Our performance studies show that ESAHR topology reduces about 40% usage of energy used during packet transmission, and is highly adaptive to the environment change. In future this topology can be equipped with route overhead endurance mechanism.

References Références Referencias

1. K. Scott and N. Bambos, “Routing and Channel Assignment for Low Energy Transmission in PCS”, ICUPC '96 , Oct. 1996
2. S. Doshi, S. Bhandare, and T. X Brown, “An Ondemand Minimal energy routing Topology for a Wireless Ad Hoc Network”, ACM Mobile Computing and Communications Review, vol. 6, no. 3 , July 2002
3. V. Rodoplu and T. Meng, “Minimum Energy Mobile Wireless Networks”, IEEE Journal on Selected Areas on Communications, vol. 17, Aug. 1999.
4. S. Banerjee and A. Misra, “Minimum Energy Routes for Reliable Communication in Multi-hop Wireless Networks”, MOBIHOC'02, June. 2002
5. J. Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, “Conserving Transmission Energy in Wireless Ad Hoc Networks”, IEEE Conference on Network Topologies, Nov. 2001
6. J. Zhu, C. Qiao and X. Wang, “A Comprehensive Minimal energy routing Topology for Wireless Ad Hoc Networks”, INFOCOM'04 , Mar. 2004
7. C. K. Toh, H. Cobb and D. Scott, “Performance Evaluation of Battery-Life-Aware Routing Schemes for Wireless Ad Hoc Networks”, ICC'01, June 2001
8. A. Misra and S. Banerjee, “MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments”, WCNC'02, Mar. 2002
9. ANSI/IEEE Std 802.11, 1999 Edition.
10. Outay, F.; Vѐque, V.; Bouallѐgue, R.; Inst. of Fundamental Electron., Univ. Paris-Sud 11, Orsay, France This paper appears in: 2010 IEEE 29th International Performance Computing and Communications Conference (IPCCC)
11. G. Bianchi and I. Tinnirello, “Kalman Filter Estimation of the Number of Competing Terminals in an IEEE 802.11 network”, INFOCOM'03, 2003
12. C-K Toh, “Ad Hoc Mobile Wireless Networks Protocols and Systems”, Prentice Hall, 2002
13. R. Schoonderwoerd, O. Holland, J. Bruten, and L. Rothkrantz. Ant-based load balancing in telecommunications networks; Adaptive Behavior, 5(2):169– 207, 1996
14. B.M.G.Prasad and P.V.S. Srinivas; IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 1, September 2012; ISSN (Online): 1694-0814

15. M. Heissenbttel and T. Braun, “Ants-Based Routing in Large Scale Mobile Ad-Hoc Networks,” University of Bern, Tech. Rep., 2003
16. D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Kluwer Academic Publishers, 1996
17. DS. PalChaudhuri and D. B. Johnson, “Power Mode Scheduling for Ad Hoc Networks”, ICNP, 2002.
18. J. Zhu and X. Wang, “PEER: A Progressive Energy Efficient Routing Protocol for Wireless Ad Hoc Networks”, INFOCOM’05 , Mar. 2005.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 15 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Authorised Secure Host Communication under Data Provenance Verification- A Signcryption Based Contract Signing Protocol

By Bolladi Swathi & P.Vasanth Sena

Sree Chaitanya College of Engineering, Karimnagar, AP,India

Abstract - The wide qualities of distributed (ex: P2P networks) network has given us many advantages and threats for enhancement of distributed computing. The best way to reduce threats is adding a reputation-based globally trusted model. Many present trust models are failing to restrain effectively some behaviors like collusive attacks, but pay no heed towards the security of this mechanism.

GJCST-E Classification : *E.3*

AUTHORISED SECURE HOST COMMUNICATION UNDER DATA PROVENANCE VERIFICATION- A SIGNCRYPTION BASED CONTRACT SIGNING PROTOCOL

Strictly as per the compliance and regulations of:

Authorised Secure Host Communication under Data Provenance Verification- A Signcryption Based Contract Signing Protocol

Bolladi Swathi [α] & P.Vasanth Sena [σ]

Abstract - The wide qualities of distributed (ex: P2P networks) network has given us many advantages and threats for enhancement of distributed computing. The best way to reduce threats is adding a reputation-based globally trusted model. Many present trust models are failing to restrain effectively some behaviors like collusive attacks, but pay no heed towards the security of this mechanism.

I. Introduction

Of late, distributed computing has become popular and well recognized in a wide range of applications, like file-sharing, digital content delivery, and distributed Grid computing [1]. But the fact remains that, peer anonymity and autonomy make distributed networks easy towards attacks by any peer who is not rust worthy. The recent works [2-5] are a benchmark to the fact that the trust theories in social networks construct well recognized trust models, to find a solution for these kinds of behaviors.

The present reputation-based trust model designs trusted rank of a peer based on its past transactions, and it's similar to the peer with full trust value is offered the role of the service provider. This method has some advantages on any malicious behaviors to a certain extent, but has a meager effect when it comes to complex attacks and when disturbances are created on these reputation systems, like collusions. The researches now a day focus on the design and working of the trust system in all sensible arenas, and barely care concerning the security difficulty it faces which can damage the tag “node consistency handling”. The security of node reliability handling is the most important element which assures a safe working of the trust management system (TMS). Thus, it is vital to develop and discuss about the security mechanism of the TMS.

Dealing by means of these research issues, we project node reliability based distributed trust model with the security mechanism that we refer as the secure node reliability information management (SNRIM), for distributed networks, which would scales better over node reliability information management(NRIM).

II. Related Work

This sector gives a wide review of some of the present distributed node reliability systems, concentrating on problems like storage and veracity. We would like to at first give an outline of the node reliability systems. Kevin A. Burton designed an open privacy distributed node reliability system [5] on p2p, which hails from the distributed trust model which brought to us the idea of node reliability network, which is made up of identities and certificates. Therefore, the certainty of the identities is appreciated from a visible sub-graph of the reputable network. P2PREP [6], which is a node reliability sharing protocol designed for Gnutella, where every peer keeps track and shares the node reliability of their peers. Reputation sharing is made by distributed polling protocol. Service requesters use this trust by polling peers. Karl Aberer et.al. [7] Made a trust managing system on the distributed system which combines the trust and data management to construct a complete distributed architecture for information systems. The node reliabilities here are expressed as complaints; higher the complaints, less trustworthy it is. After every transaction, if there is dissatisfaction, a peer files a complaint stating the problem. To examine the node reliability of a peer involves searches for complaints about the peer. Kamvar et.al [8] proposed a node reliability management system, for distributed file sharing systems such as Gnutella fighting against the spread of inauthentic file. Here, every peer has a global node reliability that shows experiences of every peer with it. Sit and Morris [9] gave an idea for security of p2p networks. Their model permits nodes to make packets with arbitrary material, but lets the nodes not to intercept arbitrary traffic. They gave taxonomy of all varied attacks and at the routing layer, they find a node lookup, routing table preservation, division the network and virtualization as threat to security. They deal also with multilevel protocols, like file storage, where nodes need not have the necessary invariants, like storage replication. They work also on denial-of-service attacks, and rapidly joining and leaving the network, or arranging for various nodes which sends bulk volumes of data to overload a

Author α : M.Tech student at Dept of CSE, Sree Chaitanya College of Engineering, Karimnagar, AP,India. E-mail : swathi.bolladi@gmail.com
Author σ : Associate Professor in Dept of Cse, Sree Chaitanya College of Engineering, AP,India.

victim's network connection (i.e., distributed denial of service attacks). Dingledine et al. [10] and Douceur [11] work on address spoofing assaults as well. Having several potentially hazardous nodes in the system and with no trusted central head which certifies node identities and become complex to know whether you can trust the claimed identity of somebody to an unknown. Bellovin [12] finds many problems with Napster and Gnutella. He discusses how complex it is to extent the use of Napster and Gnutella use via firewalls, and the ways they pass information that users feel is personal, like the search queries given. Bellovin researches also on Gnutella's "push" feature, which functions on firewalls, useful for denial of service attacks. He feels Napster's central architecture more safe against these kind attacks, even if it needs users to trust the central server. It is to be renowned that a substitute reply for secure routing table maintenance and forwarding that we denied. This answer exchanges every node by a bunch of replicas as told by Lynch et al. [13]. The replicas are run using a state machine replication algorithm like BFT [14] that can sustain faults like Byzantine. BFT can replicate arbitrary state machines and, therefore, it can look like Pastry's routing table maintenance and forwarding protocols. Here, we look into Reputation Systems for distributed networks—highly useful design which protects the distributed network without a central component, and amplifies all the advantages of the distributed network.

III. Node reliability systems

A vital corollary of a good node reliability management is the online auction system eBay [9]. Here, buyers and sellers rate each other post transaction, and the final node reliability of a contestant is the ratings he has over the last 6 months. This system depends on a central system to store and manage these ratings.

In varied areas nodes rate each other post transaction, like in eBay system. Like, every time peer I gets a file from peer j, it rates the transaction as positive (tr(i, j) = 1) or negative (tr(i, j) = −1). Peer i can rate a download as negative, if he finds the file inauthentic or tampered with, or if interrupted. Like in the eBay approach, we may possibly characterize a local faith value s_{ij} as the sum of the ratings of the individual transactions that node i has downloaded from node j: $s_{ij} = ptr_{ij}$.

Similarly, every peer i can store many transactions it has had with node j, $sat(i, j)$ and the number of intolerable transactions it has had with node j, $unsat(i, j)$. Then, s_{ij} is defined:

$$s_{ij} = sat(i, j) - unsat(i, j) \qquad (1)$$

Previous work in distributed node reliability systems [6, 1] are based on same notions of local trust values. The obstacle is in an environment is how to deal with the local trust values s_{ij} without a central storage and management. Every previous system named above finds this problem; every system proposed has a couple of negatives. It mostly averages the ratings of some nodes and has no wide view about a peer's node reliability, or it averages the ratings of the nodes and congests the network with system messages questioning for every peer's local trust values for each query.

a) *Threat Model*

A Gnutella-like network has a power-law topology and helps Insert and Search techniques. The nodes have a predefined Join & Leave protocols. The nodes are connected with a communication channel which is not secure. As the nodes have opposing interests, a motivation is required to decrease leechers. Leechers are the ones who gain benefit from the system without giving anything to the system. The rogue nodes send malware in the network. Finally, nodes judge the quality before making Go/No-Go in every transaction and develop trust relationships mutually.

A good node reliability system gives the way to achieve the target. Any node reliability system is open to ballot stuffing and bad mouthing as told in [18]. A poor node reliability system naturally gives problems that exploit the attackers. Peers should have unique way to handle to which their node reliabilities are tagged. If they are absent in trusted central agency, an attacker gathers infinite identities and gives recommendations to itself. A node can alter the reliability data in the network to uplift its node reliability and there are problems that are in the picture based on how a given node reliability system is made. We discuss those problems and their mitigation in the sections where the design decision is made.

b) *Self-Certification*

To participate in the node reliability system, a node should have handled. The reliability of a node is represented with handle. This handle is the "identity" of the node even if does not "discover" a node, i.e., it may not lead to the real-life identity of the peer. A node gets advices for every transaction, and all advices are stored together for calculation of the reliability of a node.

In a central system, the head gives these identities. In a distributed node reliability system, self-certification [33] divides the trusted entity among the nodes and gives their own identities. Every node has its own CA that gives the identity certificate(s) to the peer. All the certificates used here are same to SDSI certificates [6]. The name of a node is with its identity and the node reliability of a CA is the node reliability.

Self-certification obviates the central trusted entity for giving identities in a central system. Peers having self-certified identities are pseudononymous in the system as there isn't a way to map the identity of a node in the system to its real-life. Though anonymity or at least pseudonymity is required in distributed networks, in a node reliability system it is a double edge sword. If there is no mapping between multiple identities and the owner (peer), the system is open to Sybil attack or Liar farms.

A node uses self-certification generating many identities and raises the node reliability of identities doing false transactions. The malicious node need not collude with distinct nodes to build its node reliability, but should generate a set of identities. The set of identities managed by one node is called an identity farm. The identities issuing a false recommendation are called a liar farm. These attacks are of the class of attacks named Sybil attacks. A node having an identity farm is as powerful subverting a node reliability system as a node colluded with many of other peers.

An identity farm is countered if, a node is not allowed to one identity or all the identities of a node are sent back the peer. A node can be stopped to one identity by mapping its identity to its real-life identity and leaving anonymity, or by making the identity generation resource high that the node cannot generate more identities. Identity generated is made resource intensive by traditional micro-payment method, although the resource restrictions have a varied impact based on every peer's resourcefulness.

In self-certification, we have a combination of approaches. Every node CA gives many identities. The advices received for a peer's identity from identities of peers, signed by the other peer's CA(s), are recognized as signed by the CA, and are made to counter the liar farms. In every transaction, the requester averages all the advices of the provider by CAs of the provider's last advisors. Hence, all the past advices owned by the provider are but they get averaged. Finally, it sums up the averages of each CA calculating the node reliability of the provider identity.

Hence, a peer should not use its own identities (all generated by the same CA) to advice its other identities.

A determined peer can begin many CAs and give groups of identities. In order to oppose a rogue node with multiple CAs, the nodes are made to batches on various grounds like a node can't be a part of many groups. For example, a distributed network in a city ensures the nodes by their zip codes. Every node gets its group certificate from the required head and attaches it to its CA. The certificate of a group head is publicly used by any node inside or outside the group. The node sends its credentials to the group and the head checks and signs the group certificate.

Unlike the traditional CA or distributed CA ways, grouping of nodes has the anonymity of the peers; when grouped with self-certification it curtails the happening of a Sybil attack. In opposition to the traditional CA, neither the group head nor the transacting nodes establish the identity of the peer. The certificate revocations are not necessary in the group-based way as the group head vouches for the real-life of the peer, unlike the traditional certificate-based approaches where many certificate attributes are attested by the head and need revocation. If a good identity is adjusted, its misuses are self destructive as its node reliability will go down if misused.

The node is named P while the head is denoted by A. Here P→A: X represents that the node (P) sends a message X to the head (A), here P_{k2} stands for the private key of P and P_{k1} represents the public key of the node $P.E_k(\tau)$ represents encryption of the phrase (τ) with K, while E B_k (X) represents blinding phrase X with key K.

1. P→A:B1={E B_{ka} (I_{Alice_r})}, I_{Alice} The peer Alice gives a BLINDING KEY, K and identity for herself (I_{Alice_r}) Alice cannot be recognized from her identity (I_{Alice_r}). She also blinds her identity (I_{Alice_r}) with the blind key Ka. B1 stands for the blind identity. Alice passes B1 to the head with her real identity that approves her membership to a group.
2. A→P:B2= $E_{P_{AuthorityK2}}$ {B1=E B_{ka} (I_{Alice_r})}, I_{Alice} The head attests the blinded identity, B1 and sends it (B2) back to the peer.
3. $E_{P_{AuthorityK2}}$ {I_{Alice_r}} = E B_{ka} {B2}}The peer un blinds the signed identity and extracts the identity authorized by the head $E_{P_{AuthorityK2}}$ {I_{Alice_r}}.

The logic in the group-based way is that in a distributed network, nodes are interested in the ranks of providers than only the value of the node reliabilities. The simulations tell that this way varies the name of nodes but it having least effect on the relative ranks of the peers. This approach is from the Google page rank idea in which the pages in proximity of other don't give the page rank of the target page in the pages at a distance [34]. The relative ranks don't object the nodes from adjusting thresholds. The thresholds depend on ranks. Adjusting the thresholds for absolute values are have a limited utility. Google has ranks instead of links pointing to/from pages. It is clear from the Google corollary that rank-based mechanisms can be measured. Debates between there might be some systems needing absolute values still take place. This paper is not into that, as use of absolute values is more complex and is specific information that is not a part of our discussion.

It is opposed and supported that this way is unjustified to nodes whose authentic advice are from

Global Journal of Computer Science and Technology (E) Volume XII Issue XV Version I Year 2012

nodes that are a part of a large group. We support the argument and our implementations display that the relative ranks of the providers change the least. Hence, the providers are least influenced (Δ Mean Rank Difference≈14 for varied sizes groups) by the batches of advices. The requesters who give the advice to the providers can't be influenced by the batching of advices.

c) Node Reliability Model

The standard Join methodology is made use of by peer to connect itself to a specific distributed network. The search appeal entails the peer supplicant to produce a list of nodes who have the demanded file(s) with them. RANGE indicates the count of nodes who tender a mentioned meticulous file. The peer supplicant chooses the provider with the peak status by instigating the cryptographic procedure which involves the peer supplicant making use of the Download methodology of the network for downloading the relevant file mentioned by the client, which again assists in validating the reliability, dependability and the value of the file. A proposal is then sent to the peer client between min - recommendation and max - recommendation, which are limited to the restrictions ensuring that a single implication doesn't utterly annul or radically improve the meticulousness of a supplicant. On receiving the suggestions from the client, it averages the prior received implications and incorporates the recently received ones to estimate its repute.

The factors mentioned above can be assigned values by the means of Decision Theory, Game Theory, and Probability and function F() is identified on the basis of intensity levels of menace faced by nodes in the distributed network. The function F() in this paper is described as the arithmetic average of the suggestions that are collected by the peer supplicant. The recommended node reliability copy is self governing as compared to topology of the distributed network, nodal addressing formats, bootstrap procedures, joining and leaving protocols of the nodes present and the name service.

A negative suggestion may be issued by an applicant to the peer supplicant which may turn out to be hazardous concerning its node reliability even though the supplicant actually is worthy of a positive recommendation for a specified transaction. If in a way, only positive recommendations are accepted, then it would be tougher to distinguish between new and bad peers. Hence an assumption is made here that both positive and negative proposals are permitted and a given peer would no longer cooperate with those nodes who frequently deliver negative proposals.

d) Contract signing between peers: a signcryption approach

The entire process starts here with the employment of RSA signature algorithm [42] otherwise known as Signcryption. At this point, the 1st user divides his private key d into d1 and d2 such that $d = d1 + d2$ by following park[40]. The signature of this user has to be exchanged with the other and this signature is $\sigma_A = h(m)^{d1} \bmod n$. The partial signature generated by the 1st user is to assure that he has zero-knowledge base and this is done by Gennaro topology[27].The relations we have are defective owed to network failure or router's attacks [36],[46]. But, TTP is reliable since the messages inserted reach the destination for sure but with some delay.

i. *Registration Protocol*

The receiver of the information has only to record i.e. merely the recording process of the initiator with TTP is enough. He then gets a long-term voucher along with CA. After this, the following processes are done: (for our convenience, let the sender be BOB and receiver as ALICE.)

a. Alice first sets an RSA modulus $n = pq$, where *p* and *q* are two -bit safe primes, i.e., there exist two primes p' and q' such that $p = 2p' + 1$, $q = 2q' + 1$. After, Alice selects her random public key $e \in_R \mathbb{Z}^*_{\phi(n)}$, and calculates her private key $d = e^{-1} \bmod \varnothing(n)$, where $\phi(n) = (p-1)*(q-1)$. At last, Alice registers her public key with a CA to get her certificate C_A, which binds her identity and the corresponding pubic key (n, e) together.
b. Alice randomly splits d into $d1$ and $d2$ such that $d = d1 + d2 \bmod \phi(n)$ by choosing $d1 \in_R \mathbb{Z}^*_{\phi(n)}$, and computes $e_1 = d_1^{-1} \bmod \phi(n)$. She also generates a sample message-signature pair (ω, σ_ω), where $\omega \in \mathbb{Z}^*_n \setminus \{1, -1\}, ord(\omega) \geq p'q'$ and $\sigma_\omega = \omega^{d1} mod\, n$. Then, Alice sends $(C_A, \omega, \sigma_\omega, d2)$ to the TTP but keeps (d, d_1, d_2, e_1) secret.
c. The TTP first checks for the validation of Alice's certificate C_A. After that, the TTP checks that the triple $(\omega, \sigma_\omega, d2)$ s arranged correctly. If the whole thing is in exact order as per its rules, TTP saves d2 and generates a voucher V_A by computing $V_A = Sign_{TTP}(C_A, \omega, \sigma_\omega)$. This proves the TTP's signature on message $(C_A, \omega, \sigma_\omega)$, which guarantees that the TTP can issue a valid partial signature on behalf of Alice by using the secret $d2$.

ii. *Signature Exchange Protocol*

Before all this, a contract has to be agreed between bob and Alice and they should sign it. It should also has a deadline, and identify the Alice, Bob, and TTP.

a) Initially, the initiator Alice has to compute her partial signature $\sigma_1 = h(m)^{d1} \bmod n$, and then sends the triple $(C_A, \omega, \sigma_\omega)$ to the responder Bob. Here, $h(.)$ is a cryptographically secure hash function.

b) After receiving (C_A, V_A, σ_1), Bob first verifies that C_A is whether issued by CA, and V_A is Alice's voucher created by the TTP. Then, Bob checks if the identities of Alice, Bob, and the TTP are correctly mentioned as part of the contract '*m*'. If all these checking are ok, Bob initiates the below interactive zero-knowledge protocol with Alice to check whether σ_1 is Alice's valid partial signature on contact.

   i. Then Bob selects two numbers $i, j \in_R [1, n]$ at random, and a challenge c to Alice is sent by computing $c = \sigma_1^{2i} \sigma_w^{\ j} \bmod n$.

   ii. Receiving the challenge c, Alice calculates the response $r = c^e \bmod n$ She then returns her commitment $\bar{r} = TCcom(r, t)$ to Bob using a random number t, where $TCcom$ is the commitment algorithm.

   iii. After receiving the commitment $\bar{r}$, Bob sends Alice the pair (i, j) to acknowledge that he is done with the challenge c properly.

   iv. Alice verifies for correct preparation of c, that is $c \equiv \sigma_1^{2i} \sigma_\omega^{j} \bmod n$. If ok, Alice withdraws his commitment $\bar{r}$ by knowing the responses (r, t) to Bob. With this (r, t), Bob knows σ_1 as valid if and only if $r \equiv h(m)^{2i} \omega^j \bmod n$ and $\bar{r} \equiv TCcom(r, t)$.

c) Bob checks the σ_1 Alice's valid partial signature and the deadline t mentioned in contract m is whether enough for resolving the dispute resolution from the TTP. Then only he sends his signature σ_B to Alice.

d) After receiving σ_B, Alice has to check whether it is Bob's valid signature. If it is, she sends Bob the partial signature σ_2 by computing $\sigma_2 = h(m)^{d2} \bmod n$. As Bob receives σ_2, he sets $\overline{\sigma_A} = \sigma_1 \sigma_2 \bmod n$, and accepts σ_2 as valid if and only if $h(m)^2 = \overline{\sigma_A}^{2e} \bmod n$. Here, Bob can receive Alice's standard RSA signature σ_A on message m from $\overline{\sigma_A}$. If all this do not happen, Bob seeks the help of TTP for connection before the expiry of the date.

IV. Node reliability exchange protocol

The status swapping procedure is commenced with the node supplicant when the node applicant chooses the supplicant with the highest status. This procedure requires the applicant to be represented as R and the node supplicant is represented as P. As in R→P: X represents that the node sends a message X to the supplicant (P).denotes private key of node P while P_{k1} denotes public key of the peer $P.E_k(\tau)$ denotes encryption of the phase (τ) with key K and E B_K (X) symbolizes blinding phrase with a key K. H(λ) denotes a one way hash of the value λ. This procedure supposes that obtainable functions are inserting and search, but are not flexible enough for nodes which may not be proposed tag along the join and leave procedures of the network. The status swapping procedure contains the following phases:

Step 1: R→P: RTS & IDR a REQUEST FOR TRANSACTION (RTS) is sent by the node applicant along with its own IDENTITY CERTIFICATE (IDR) to the node supplicant as it is required for authentication purposes in Step 7.

Step 2: P→ R: IDP & TID & $E_{p_{k2}}$ (H(TID)‖RTS . The peculiar IDENTITY CERTIFICATE (IDP), the CURRENT TRANSACTION ID (TID) and the signed TID, $E_{p_{k2}}$ (H(TID)‖RTS is sent by the node supplicant wherein signed TID is essential for the supplicant to avoid duplication of the usage of the same transaction id again. The applicant also applies for this signed TID and piles it up in the network at the end of the procedure for admission to other peers.

Step 3: R : LTID (Max (Search(PK1‖ TID)). The value of the LAST TRANSACTION ID (LTID) that was used by the supplicant is gathered by the node applicant who then combines the public ke P of the node supplicant along with the string TID and a search operation is carried out. Any node present in the network responds only when it has the relevant TID that is specified by the applicant and the node applicant chooses the highest TID out of all the TIDs received. The highest TID value becomes the LTID. It is certainly possible that the node supplicant may conspire with the node who piled up its last LTID and may modify it, but this is impossible as the applicant registers relevant information.

Step 4: R : IF(LTID≥ TID)GO TO Step 12 Foul play is presumed if the value of LTID initiated by the node applicant is originally from some other random transaction and applicant jumps to Step12.

Step 5: R→P: Past Recommendation Request & r. If the step 4 check gives successful results, then applicant requests the supplicant for the earlier received proposals. If the current transaction being performed is, say Nth transaction, the applicant makes a head-on request for N-1th,N-2th,….,N-nth proposals where r<N. The node applicant is solely responsible for deciding the value of r and is considered to be directly proportional to the applicant's venture in the transaction.

Step 6: P→R: CHAIN, $E_{p_{K2}}$ (CHAIN)

CHAIN=({RE C_{N-1} ‖ EZ_{N-1K2} (H(RE C_{N-1}))}‖

{RE C_{N-2} ‖ $E_{Z_{N-2K2}}$ (H(RE C_{N-2} ,RE C_{N-1}))} ‖

{RE C_{N-3} ‖ $E_{Z_{N-3K2}}$ (H(RE C_{N-3} ,RE C_{N-2}))}‖

{RE C_{N-4} ‖ $E_{Z_{N-4K2}}$ (H(RE C_{N-r} ,RE C_{N-r-1}))})

The earlier received proposals RE C_{N-1} , RE C_{N-2},……, RE C_{N-3} which were provided by nodes $Z_{N-1}, Z_{N-2}, \ldots.., Z_{N\ 3}$ .is sent by the supplicant. The CHAIN is singed so as to enable the applicant to hold supplicant responsible for the chain. The supplicant can, in no way, change the proposals that have been assessed by the earlier applicants. Consider an applicant (say Z_1) has signed both the (ı th) and the previous (ı -1th) recommendation using its private key Z_{K2}, as $E_{Zn_{K2}}$ (H(RE C_{N-3} ‖ RE $C_{N-(\iota-1)}$)), in no way can a supplicant alter the CHAIN.

Step 7:R : Result=Verify(RE C_{N-1} ;RE C_{N-2} RE C_{N-r})

If Result != Verified GO TO STEP 12

A simple public key cryptography protocol is employed by an applicant to authenticate the CHAIN. The authentication process is easier when a supplicant possesses certificates of all the nodes with whom it had connections earlier. In case it doesn't have one, it accumulates it from the supplicant itself. The provider had obtained its requester's certificate in Step 1. Liar farms (specified in Section 3.2, paragraph 2) are checked for by the applicant. The applicant jumps to Step 12 in case the authentication process fails.

Step 8: Contract signing between node selected under node reliability check and node that requesting the service

Signature exchange protocol will get into action between Peer "SRP" that requesting the service and Peer "SPP" that selected as service provider by node reliability check.

Initially, the initiator SRP has to compute her partial signature $\sigma_1 = h(m)^{d1} \bmod n$, and then sends the triple $(C_A, \omega, \sigma_\omega)$ to the responder SPP. Here, $h(.)$ is a cryptographically secure hash function. After receiving (C_A, V_A, σ_1), SPP first verifies that C_A is whether issued by CA, and V_A is SRP's voucher created by the TTP. Then, SPP checks if the identities of SRP, SPP, and the TTP are correctly mentioned as part of the contract 'm'. If all these checking are ok, SPP initiates the below interactive zero-knowledge protocol with SRP to check whether σ_1 is SRP's valid partial signature on contact. Then SPP selects two numbers $i, j \in_R [1,n]$ at random, and a challenge c to SRP is sent by computing $c = \sigma_1^{2i} \sigma_w^{\ j} \bmod n$. Receiving the challenge c , SRP calculates the response $r = c^e \bmod n$ She then returns her commitment $\bar{r} = TCcom(r,t)$ to SPP using a random number t, where $TCcom$ is the commitment algorithm. After receiving the commitment $\bar{r}$, SPP sends SRP the pair (i, j) to acknowledge that he is done with the challenge c properly. SRP verifies for correct preparation of c, that is $c \equiv \sigma_1^{2i} \sigma_\omega^j \bmod n$. If ok, SRP withdraws his commitment $\bar{r}$ by knowing the responses (r,t) to SPP. With this (r,t) , SPP knows σ_1 as valid if and only if $r \equiv h(m)^{2i} \omega^j \bmod n$ and $\bar{r} \equiv TCcom(r,t)$. c). SPP checks the σ_1 SRP's valid partial signature and the deadline t mentioned in contract m is whether enough for resolving the dispute resolution from the TTP. Then only he sends his signature σ_B to SRP. After receiving σ_B, SRP has to check whether it is SPP's valid signature. If it is, she sends SPP the partial signature σ_2 by computing $\sigma_2 = h(m)^{d2} \bmod n$. As SPP receives σ_2, he sets $\overline{\sigma_A} = \sigma_1 \sigma_2 \bmod n$, and accepts σ_2 as valid if and only if $h(m)^2 = \overline{\sigma_A}^{2e} \bmod n$. Here, SPP can receive SRP's standard RSA signature σ_A on message m from $\overline{\sigma}_A$. If all this do not happen, SPP seeks the help of TTP for connection before the expiry of the date.

Step 9: P→R : File or Service

The file or service is afforded as per the obligation specified concerning search operation performed for the supplicants.

Step 10: R →P : B1 =E B_{Ka} (REC‖ TID‖ $E_{R_{K2}}$ {H(REC, ‖ TID)})

A BLINDING KEY (Ka) is produced by an applicant on receiving the service, who then combines the RECOMMENDATION (REC) and the TRANSACTION ID (TID) it had received in Step 2 and signs it. Consequently, the signed proposal is blinded along with the blinding key, Ka. This is done in order to entrust the supplicant to the proposal received before it actually knows the value, lest it disowns it on recognizing that it is low. It is also involves the fact that the supplicant made use of TID in a blinded suggestion from the node applicant, which is also authenticated by the applicant itself. The blinded proposal includes the Chain that is consequently used by the supplicant to certify its status to some other applicant.

Step 11:

a. P →R : B1|| $E_{P_{K2}}$ (H(B1),nonce),nonce

b. R→P : Ka

A NONCE is sent by the supplicant after signing the proposal even though it is unable to see the proposal and acknowledges it back to the applicant, who then authorizes the signature and sends blinding key Ka to the supplicant to unblind the received string in Step10a and confirms the received proposal.

Step 121: Insert

(IDR;{REC ||TID|| $E_{R_{K2}}$ {H(REC) || H(TID)}})

The proposal assigned to the supplicant (REC), the transaction id (TID), and its own identity certificate is verified by the applicant and is then accumulated in the network using Insert methodology of the distributed network which marks the end of the transaction.

Step 13: Step 12 is concerning the methodology executed by an applicant when foul play is anticipated.

ABORT PROTOCOL

R: Insert (IDR; {CHAIN ||TID|| $E_{R_{K2}}$ {H(CHAIN) || H(TID)}})

If the authentication process in Step7 fails, the applicant takes the CHAIN that was verified b the supplicant and also the TID is taken into consideration after which, it is signed and the Insert methodology is preferred to be made use of to insert the chain and also its own identity certificate into the network. Subsequently, any suitable applicant wil be able to confirm with the statistics of the failed authentication efforts and a MIN RECOMMENDATION for that TID is presumed for the supplicant. Fafe proposals cannot be encouraged to be inserted into the network as TID is to initiated that is verified by the supplicant. If an applicant reaches Step 12 from Step 4 without any possible hindrances, it will then apply for the Chain form the supplicant and will then afterward execute

$$R: \mathrm{Insert}(\mathrm{IDR},\{\mathrm{CHAIN} \| \mathrm{TID} \| \{H(\mathrm{TID} \| \mathrm{RTS}))\}\}) .$$

V. Analysis of the protocol

Only a single search request is supposed to be commenced in the network so as to gather the already received proposals that were previously received by the supplicant. Also able to prevent the tampering node reliability provided by SRP to SPP by nodes that in path. This process is required the accountability of tackling the issue of unbalanced nature of availability of nodes in the network, which is measured to be a main subject concerning distributed networks.

1. The supplicant unintentionally forwards the wrong TID in Step 2. Consider that id which the supplicant forwards as TID and the LTID be the last Transaction ID for the supplicant. The value of TID is always supposed to be equivalent to LTID + 1. If in case of TID' > LTID+1, there arises a situation wherein there will be inexplicable misplaced proposals. If again in case of TID' < LTID+1, then the supplicant will be caught up with in the Step 4 of the procedure, as the last id issued and used by the supplicant was made public and accessible to all the peers. The value of TID is considered as 0 if a node is for the first time donning the role of a supplicant.
2. The transaction in Step 8 will not be terminated by the supplicant. A supplicant is allowed to abandon the transaction after providing the applicant with the requested requisite information in Step 8 and also can abandon the transaction after Step 9. In both the cases, there is an absence of a proposal by the supplicant for the transaction id TID. The proposal in Step 11 can be liberated by the applicant provided the supplicant fails to verify and sign the blinded proposal, without acquiring the supplicant's signature. In the next transaction, precisely TID+1, the supplicant again fails to illustrate the proposal for that relevant transaction, TID to the transaction's applicant, TID+1 and hence the new applicant entrusts itself with the job of scanning the network making use of Search methodology for TID. In case TID is found, the suggested proposals are also found out pertaining to the suppliant in the transaction. The applicant will then be responsible as the TID would by then have been signed b the supplicant, who will have to acknowledge the proposal as it comprises the signature of the supplicant, TID & $E_{P_{K2}}$ (H (TID)). A minimal suggestion TID is presented to the supplicant by the node applicant in the absence of the availability of the required proposal. If in Step 10, the supplicant acknowledges the signed blinded proposal B1 & $E_{P_{K2}}$ (H (B1)), the applicant refuses to send the key, Ka and directs itself to Step 10, missing all the requisite steps, and then the supplicant scans the entire network and acquires the verified proposal of

the applicant. If an applicant skips or fails to execute Step 10, then in the upcoming transaction TID+1, LTID is looked for by the new applicant and fails in his endeavor. Hence, TID can be considered as terminated and the next transaction can be continued with the transaction id provided, TID.

3. Collusion by rogues or liar farms. All status systems are prone to complicity on account of its nature. It is possible for two or more liar farms to combine and conspire in order to augment each other's status. The influence of the conspiracy can be alleviated by classifying proposals on the basis of personage *identities*, substantiating agencies etc. The list of conspirators can be circulated, thereby, guarding the remaining nodes from an possible attack. Peers when recognized as conspirators will not be permitted to get back into the stream of network and hence they have an impetus next to conspiracy. The series of proposals of the plotters will aid in offering support that few nodes are conspiring, thereby, protecting good nodes and from the intrusion of bad nodes into the network.
4. Multiple requesters and concurrency. A supplicant in the presently used procedure will not be provided with the facility of making use of the same identity in the synchronized communication. The first option for process intensification is that the supplier identifies and familiarizes all its applicants with each other. As a result, the verification process performed in Step 4 is performed amidst a group of applicants and results are arranged in accordance with the fact that TID dissimilarity needs to be initiated due to more number of applicants. After integrating the augments, there would be a bi party procedure that would still be prevalent where the cluster of applicants is considered to the second party while the supplicant is supposed to be the first party. The figure 1 explores the ability of the proposed model to prevent the false node reliability submitted by unauthorized nodes that acts as a service request node SRP.

We can observe that contract signing by signcryption approach is most effective to prevent the node reliability tampering attacks. Even node communication with contract signing also victimized few times but victimization occurred due to contract signing breakage. Hence if contract sign is alive then attacked to tamper the node reliability is almost null. The figure 2 confirms the stable growth in execution time when considers this contract signing process, which was compared with node communication process without contract signing.

Hike at node communication execution time that is negligible when consider the improvement in prevention of node reliability tampering attack attempts.

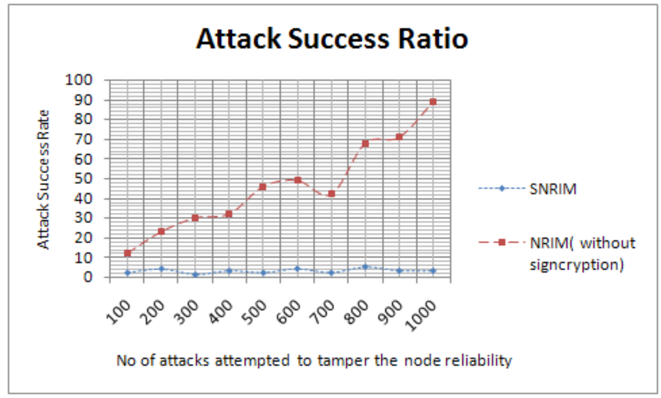


Fig. 1 : Attack success rate on NRIM and SNRIM

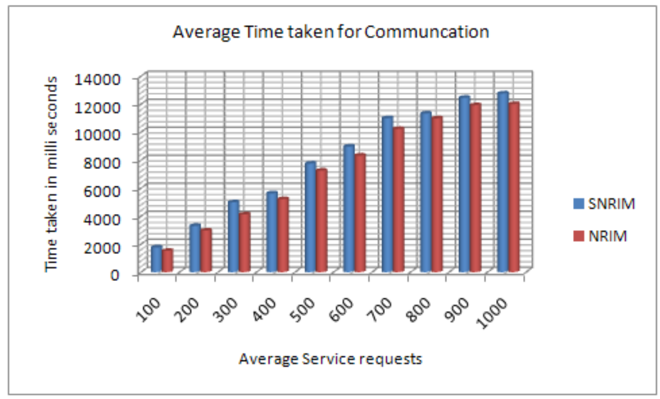


Fig. 2 : Average time taken to finish service request in SNRIM and NRIM

VI. Conclusion

Here in this paper we proposed a signcryption based contract signing for node communication based on node reliability check. The results are evident that proposed two way node reliability checking model is effective to avoid the node reliability tampering attack efforts. The planned model is screening a little hike in average process time of node communication, which can be negligible in the context of node reliability tampering attack avoidance. In future we plan to find a solution to avoid the contract sign breaching.

References Références Referencias

1. M. Ripeanu, I. Foster, and A. Iamnitchi, \Mapping the Gnutella network: Properties of large-scale peer-to-peer systems and implications for system design," IEEE Internet Computing Journal, vol. 6, no. 1, 2002.
2. S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, \A scalable content addressable network," in ACM SIGCOMM, Aug. 2001.
3. I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan, \Chord: A scalable Peer-To-Peer lookup service for internet applications," in ACM SIGCOMM, Aug. 2001, pp. 149{160.

4. E. Adar and B. A. Huberman, \Free riding on Gnutella," Tech. Rep., Xerox PARC, 2000.
5. S. Saroiu, P. K. Gummadi, and S. D. Gribble, \A measurement study of peer-to-peer sharing systems," in SPIE Conference on Multimedia Computing and Networking (MMCN), Jan. 2002.
6. K. Aberer and Z. Despotovic, \Managing trust in a peer-2-peer information system," in Ninth International Conference on Information and Knowledge Management (CIKM), Nov. 2001.
7. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, \A reputation-based approach for choosing reliable resources in peer-to-peer networks," in 9th ACM Conference on Computer and Communications Security, Nov. 2002.
8. S. D. Kamvar, M. Schlosser, and H. Garcia-Molina, \Eigenrep: Reputation management in p2p networks," Unpublished work, 2003.
9. S. Lee, R. Sherwood, and B. Bhattacharjee, \Cooperative peer groups in nice," in IEEE INFOCOM, Apr. 2003.
10. L. Xiong and L. Liu, \Building trust in decentralized peer-to-peer communities," in International Conference on Electronic Commerce Research (ICECR-5), Oct. 2002.
11. \Gnucleus home page," http://www.gnucleus.com/.
12. K. Sripanidkulchai, \The popularity of gnutella queries and its implications on scalability," White Paper Featured on O'Reilly's website http://www.openp2p.com/, Feb. 2001.
13. J. Chu, K. Labonte, and B. N. Levine, \Availability and locality measurements of peer-to-peer le systems," in ITCom: Scalability and Trac Control in IP Networks. July 2002, vol. 4868 of Proceedings of SPIE, Proceedings of SPIE.
14. \Kazaa participation level," http://www.kazaa.com/.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 15 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

GSM Based Operating of Embedded System Cloud Computing, Mobile Application Development and Artificial Intelligence Based System

By Prashant Kumar, Dr. Suyash Narayan Mishra & Zoheb Rahman

Amity University, Lucknow

Abstract - The purpose of this paper is to identify and explore the challenges for potential solutions in the field of Mobile Application, Cloud Computing, Artificial Intelligence, Robotics and Home – made Devices (Television, Refrigerator, Air Conditioner, Air Cooler, Mixer Grinder) in Embedded Systems. This paper is an attempt to introduce the reader into the world of GSM based Operating of Embedded Systems in voice based talking GSM technology and its applications (for updating the new technologies in old device) in the industry of home – made appliances and devices in Embedded Systems.

The objective of the series will be a general discussion of GSM based new operating technologies for Mobile Applications Development and Mobile Computing in terms of Artificial Intelligence. Its application will working from non – mobile devices in home - made appliances and robotics.

Keywords : Cloud Computing, Mobile Application Development, Artificial Intelligence, Embedded Systems, Robotics, Home – Made Appliances.

GJCST-E Classification : C.3

GSM BASED OPERATING OF EMBEDDED SYSTEM CLOUD COMPUTING, MOBILE APPLICATION DEVELOPMENT AND ARTIFICIAL INTELLIGENCE BASED SYSTEM

Strictly as per the compliance and regulations of:

GSM Based Operating of Embedded System Cloud Computing, Mobile Application Development and Artificial Intelligence Based System

Prashant Kumar [α], Dr. Suyash Narayan Mishra [σ] & Zoheb Rahman [ρ]

Abstract - The purpose of this paper is to identify and explore the challenges for potential solutions in the field of Mobile Application, Cloud Computing, Artificial Intelligence, Robotics and Home – made Devices (Television, Refrigerator, Air Conditioner, Air Cooler, Mixer Grinder) in Embedded Systems. This paper is an attempt to introduce the reader into the world of GSM based Operating of Embedded Systems in voice based talking GSM technology and its applications (for updating the new technologies in old device) in the industry of home – made appliances and devices in Embedded Systems.

The objective of the series will be a general discussion of GSM based new operating technologies for Mobile Applications Development and Mobile Computing in terms of Artificial Intelligence. Its application will working from non – mobile devices in home - made appliances and robotics.

Keywords : Cloud Computing, Mobile Application Development, Artificial Intelligence, Embedded Systems, Robotics, Home – Made Appliances.

I. Introduction

With the advancement in technology [1]we can create and developing the new technologies in the operating of mobile application development in non – mobile devices. The technologies of Information Technology are also fast developed in the field of Mobile Communication and Field of Electronics.

There are various technologies present which become to easier the daily life of human people. This paper is an idea for making and giving the operating features of embedded systems through Mobile Computing and Mobile Application Development [1,5] by using the concept of Artificial Intelligence. This concept was used for controlling the embedded systems in Robotics and Home Made Appliances. The application of this project [1] in terms of paper has given a new generations of home - made devices in mobile application of cloud computing.

II. Principle

The project of this principle is used for controlling the embedded systems through taking the application of Robotics and Home – Made Appliances. This principle is also useful for controlling the home – made appliances and robots through voice talking based GSM Technology [3] with updating the new technologies in old devices for making the WAP connection through cloud computing [4] for operating the system. This technology is also useful for developing the principle of Artificial Intelligence at the updating of new technologies. The positive effect of this point is useful for less repairing and automatic mode repairing [2] of embedded systems, robotics and home – made appliances through updating the device or cloud computing system. This principle also gives the High Speed Internet Connectivity [1] through Cloud Computing System. This technology will also helpful for increased production [2] of home – made appliances in developing countries.

III. Practical applications

This is the project for generating the concept of cloud computing [1] through the updating of various devices like Television, Refrigerator, Air Conditioner etc. and getting the High Speed Internet Connectivity for another devices. This project also generates the [4] concept of Artificial Intelligence through by giving the concept of Automatic Mode Repairing or Updating of various devices like Television, Refrigerator, Air Conditioner etc. It also generates the concept of Mobile Application Development through our devices in Embedded Systems. We have wanted to make a two Embedded Systems:-

1. Server
2. Client

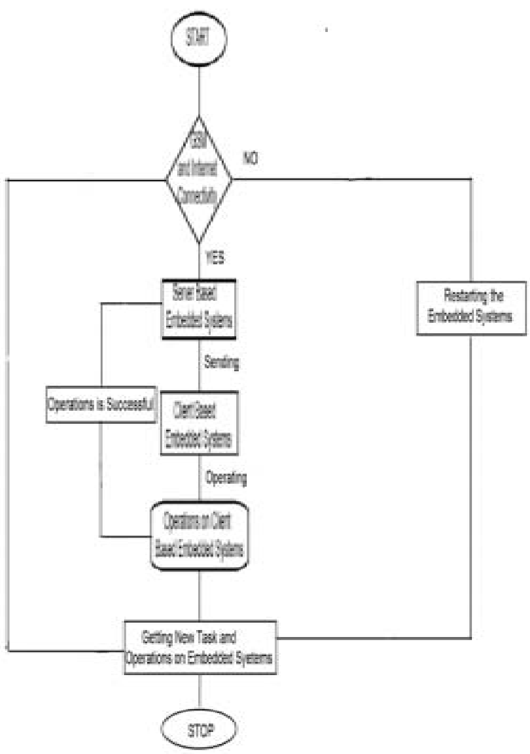
Both of these two systems are connected through Internet Connectivity by using the concept of [1] ABP Software or any Internet Coding Software in Embedded Systems.

Author α : B.Tech. Scholar at Amity School of Engineering and Technology in Amity University, Lucknow.
Author σ : Assistant Professor at Amity School of Engineering and Technology in Amity University, Lucknow.
Author ρ : B.Tech. (M.E.) at Bengal College of Engineering and Technology, West Bengal University of Technology.
E-mails : kumar.prash3@gmail.com, drsnm2010@gmail.com, zuvicks@gmail.com
Official E-mails : prashant.kumar2@student.amity.edu, snmishra@lko.amity.edu

When we will send any information to the client through server based Embedded Systems. The server information will reach and operation will perform to the client based Embedded Systems. When the operations will have performed, the client based Embedded Systems will send the message through server to "Operation is Successful."

So, both the client and server embedded systems are to be connected in High Speed Internet Connectivity and GSM Communication Systems. This project also gives the concept of Automatic Mode Repairing [2] and Updating of New Technologies in various devices based Embedded Systems. This is the technology for designing the embedded system [1] in Television, Refrigerator, Air Conditioner and various devices. This Embedded System also giving the applications of Robotics System. This system enables:

1. Any Mobile Phone is not using in our project for making GSM Communication Systems.
2. It also requires two Embedded Systems connected through the Internet Connectivity and GSM Communication Systems
3. LCD's are also available for both making the Client and Server based Embedded Systems.



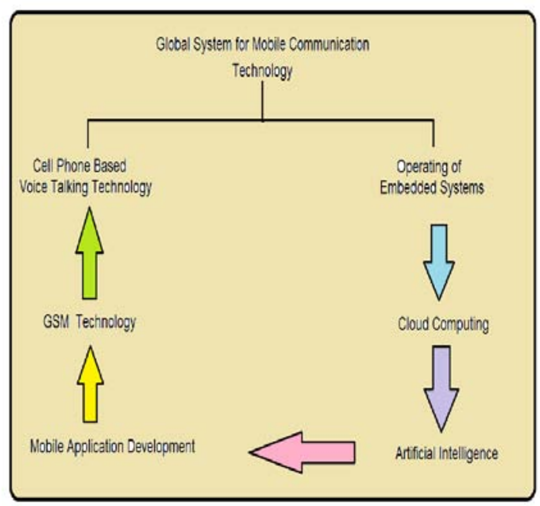
Flow Chart Diagram of Embedded System

This Embedded System has giving the future applications of Home-made Appliances for designing and updating the system. Although this application is possible in Robotics System and Home- Made Appliances. This technology has also used in Mobile and Cell Phone Industries. It has reduced the Cell Phone Radiation through Cloud Computing System. This technology also gives the free High Speed Internet Connectivity and Internet Phoning for Home – Made Appliances. The concept arises for the best idea and few years of research in GSM technologies for Home-made Appliances.

IV. GSM Networking Architecture

The GSM Networking indicates that Global System for Mobile Communication Networking. This architecture represents the many features and applications on daily life of human people. GSM is a digital mobile telephony system [1,9] that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA) and it is the most widely used of the three digital wireless telephony technologies (TDMA, GSM and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of data for making the communication. It operates at either [1] the 900 MHz or 1800 MHz frequency band. This networking architecture is also useful and connects the devices with million distances of the world. This networking architecture also connected to the many users and millions of devices.

Networking Architecture of GSM Based Operating of Embedded System



V. Cloud Computing

Cloud Computing refers to the delivery of computing and storage capacity [6,7] of a service. The name comes from the use of clouds as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software and computation [5] over a network. It has considerable overlap with software as a service. Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network.

The cloud computing also connects and establishes the network of operating many devices [1] through a server access portal. This technology is also making the cloud for controlling and operating the many devices.

VI. Mobile Application Development

It is the process by which application software is developed for low-power handheld devices [6] such as personal digital assistants, enterprise digital assistants or mobile phones. These applications are either pre-installed on phones during manufacture, can be downloaded by customers from various mobile software distribution platforms, or web applications delivered over HTTP which use server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a Web browser. The mobile application is very useful [10] and developed in the operating of mobile phones. The mobile application is very famous for generating the new technologies and operating features of mobile device.

VII. Artificial Intelligence

It is the intelligence of machines and the branch of computer science [3] that aims to create it. It defines the field as "the study and design of intelligent agents" where an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. Artificial intelligence has been the subject of optimism, but has also suffered setbacks and, today, has become an essential part of the technology industry, providing the heavy lifting for many of the most difficult problems in computer science. This device is the basic principle of Artificial Intelligence. The Artificial Intelligence is also useful for developing his sense [4] in any system of machine. This project is also developing the artificial intelligence for giving the updating of new technologies through which it become automatic mode repairing in home – made device and embedded system.

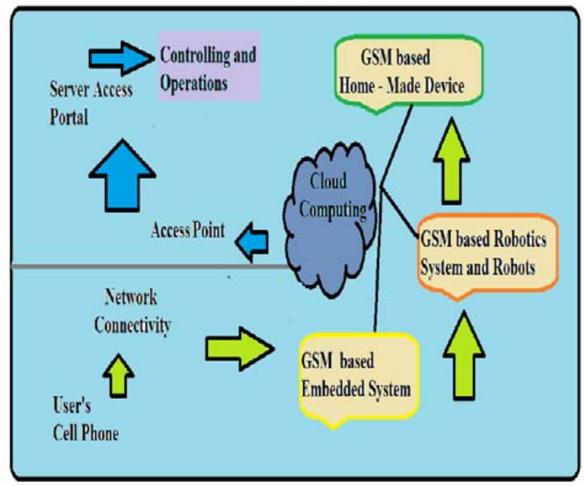
VIII. Working in Embedded System

The project of this paper is to make a wireless GSM connection [1] in between user and embedded system of home - made devices (Television, Refrigerator, Air Conditioner etc) and Robotics.

This device presents a sensor from Artificial Intelligence for controlling of Embedded Systems in Voice Talking Technology based GSM System. This technology developed a new generation for developing WAP connection on cloud computing [7,8] with operations of home – made devices. Its application is important for updating and controlling the operations or work processing of home – made devices. This GSM technology based device is developing the many work stage in operating the Embedded System by making the main application of homemade appliances.

These work stages include:

a) To establish the GSM connection in Embedded Systems.
b) To establish the voice talking technology based GSM system.
c) To establish the cloud computing for controlling the operation of Embedded Systems.
d) To establish the WAP connection for updating the operation of mobile application in home – made appliances through Mobile Cloud Computing.

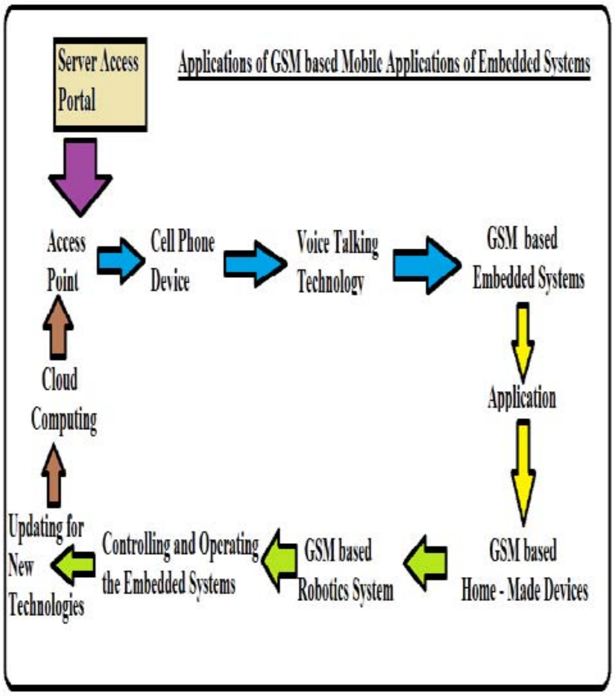


Working Process of GSM based Operating Embedded System

IX. Application

The applications of this project in terms of research paper developed a new technology for using the mobile application development [6] in non – mobile devices like Robotics and Home – Made Devices. This technology developed the operations of current – voltage power supply, controlling and operating the all parts and connecting through new technologies. Used Applications of home – made devices in Television, Refrigerator, Air Conditioner, Air Cooler, Mixer Grinder is controlling all the parts and current – voltage power supply for establishing the cloud computing [7] in various devices of networks. This technology will also developing the principle of Artificial Intelligence for operating and automatic mode repairing in home – made appliances and embedded system.

Global Journal of Computer Science and Technology (E) Volume XII Issue XV Version I Year 2012



X. Embedded Systems

An Embedded System is a computer designed system for specific control function within a larger system [2] often with real time computing constraints. It is embedded as a part of completed device often including hardware and mechanical parts. Embedded Systems [8] control many devices in common use today. Embedded Systems contain processing cores that are typically either Microcontroller or Digital Signal Processor. The designing of Embedded Systems is to make a computer through computing of device.

XI. Robotics

The world we interact in everyday and the technology that we [9] utilize are making the new technology of Robotics in Embedded System. The Robotics System provides the engineering foundation for the design, implementation and analysis of embedded system with an emphasis in autonomous robotics system. It creates the many features [10] of mechanical design, control electronics, embedded programming machine and adaptive programming development.

"The technology for an automatic device that perform functions normally describe to human or a machine in the form of human people."

XII. Home – Made Appliances

The Home – Made Appliance are using in home and easy the daily work of human people. Home – Made Appliances also become the easier and comfortable life of human people. The work applications [4] of home – made appliances:

a) Television gives the World of Entertainment.
b) Refrigerator gives the preservation of food, making ice and cold water.
c) Air Conditioner gives the cold room at longer time.
d) Air Cooler gives the cool air in every season of time.
e) Mixer Grinder gives the various spices for grinding and many things.

XIII. Conclusion

There are various technologies developed in the field of electronics and mobile application development. This paper is an attempt for developing the application of mobile in embedded systems. This technology will also useful for making the mobile application based home – made appliances by giving the [3] controlling principle of Artificial Intelligence. This principle is also useful for robotics through cloud computing [7] in which user can already access his robot through cloud computing. The application of mobile in robotics system is operating the function of robots. It will also give the concept of Artificial Intelligence for operating and updating the Embedded System.

This technology is also give the concept of GSM Based Controlling Device through Voice Talking Technology [1] in which human people is connecting and controlling the operation of electronic device [2] and home – made appliance with any part of the world. This paper is introducing the concept of computer based technology in Home – Made Appliances (Television, Refrigerator, Air Conditioner, Air Cooler and Mixer Grinder) and Robotics System. This technology will also give its application and future aspects of computer based home – made appliances in embedded system.

References Références Referencias

1. Prashant Kumar, Professor (Dr.) O.P. Singh "Recent Trends in Mobile Communication", Evaluation of Term Paper, June 2012, Amity University Uttar Pradesh Lucknow Campus.
2. Prashant Kumar, "Piezo Electricity Generations & Its Devices", Volume -2, Issue – 3, July 2012, International Research Journal of Humanities, Engineering and Pharmaceutical Sciences.
3. Nick Bostrom, Eliezer Yudkowsky, "The Ethics of Artificial Intelligence", Cambridge Handbook of Artificial Intelligence, Cambridge University Press, 2011.
4. Markus Weiss, Adrian Helfenstein, Friedemann Mattern, Thorsten Staake, "Leveraging smart meter data to recognize home appliances."
5. David Burford, "Cloud Computing: A Brief Introduction", LAD Enterprizes, 2010.
6. Vini Madan, S.R.N. Reddy, "GSM-Bluetooth based Remote Monitoring and Control System with

Automatic Light Controller", Volume – 46, No. – 1, May 2012, International Journal of Computer Applications.

7. Rob Lovell, White Paper: "Introduction to Cloud Computing", Think Grid.
8. Parineeth M Reddy, "Embedded Systems", December 2012, Resonance.
9. Jayanta Kumar Pany, R.N. Das Choudhury, "Embedded Automobile Engine Locking System,
10. Using GSM Technology", Volume- 1, Issue – 2, 2011, International Journal of Instrumentation, Control and Automation.
11. Abid Khan, Ravi Mishra," GPS – GSM Based Tracking System", Volume – 3, Issue – 2, December 2012, International Journal of Engineering Trends and Technology.

Global Journals Inc. (US) Guidelines Handbook 2012

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.

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.

MANUSCRIPT STYLE INSTRUCTION **<u>(Must be strictly followed)</u>**

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 .

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

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