Journal of Mobile Communication and Networking

Volume No. 12

Issue No. 2

May - August 2024

ENRICHED PUBLICATIONS PVT.LTD

JE - 18,Gupta Colony, Khirki Extn,
Malviya Nagar, New Delhi - 110017.
E- Mail: info@enrichedpublication.com
Phone :- +91-8877340707

Journal of Mobile Communication and Networking

Aims and Scope

Journal of Mobile Communication and Networking welcomes the original research papers, review papers, experimental investigations,surveys and notes in all areas relating to software engineering and its applications. The following list of sample - topics is by no means to be understood as restricting contributions to the topics mentioned.

Journal of Mobile Communication and Networking

Journal of Mobile Communication and Networking

(Volume No. 12, Issue No. 2, May - August 2024)

Contents

Survey: Authentication and Key Distribution Schemes for Wireless Sensors Network

Shweta Goel, Manjeet Behniwal, Ajay Kumar Singh
Department Of Computer Science Engineering, Ambala College of Engineering & Applied Research, Devasthali, Ambala City, India

ABSTRACT

Wireless sensor network contains sensor nodes having limited capabilities to sense, collect, and manipulate the data. The sensed data often need to be sent back to the base station for analysis. However, the sensing field may be too far from the base station. This may cause the transmission of data over long distances using multi-hop which may weaken the security strength. There may be different types of attack. These attacks can modify the sensed data by capturing the intermediate nods. Therefore, security services, such as, authentication and key establishment between sensor nodes, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. In this paper we will review the security threats and various key distribution techniques. These techniques can be used to secure the sensor network.

Keywords - Attacks, Cryptography, Key distribution, Security, Wireless sensor networks

1. INTRODUCTION

Wireless sensor network is one of remarkable technologies for ubiquitous computing environment to enable an end-user to gather the nearby context information. Typical examples of this network are location supporting application for indoor environment and environment monitoring application. In these applications, user mobility should be considered in authentication process. However, the existing approaches do not considered this issue. Node should perform authentication procedure again after the node moves another position. [11][12]

SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

Security challenges in WSN are as follows:

1. Minimizing resource consumption and maximizing security performance.
2. Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
3. In-network processing involves intermediate nodes in end-to-end information transfer.
4. Wireless communication characteristics render traditional wired-based security schemes unsuitable.

5. Large scale and node mobility make the affair more complex.
6. Node adding and failure make the network topology dynamic. [12]

ATTACKS ON WIRELESS SENSOR NETWORK

Active Attack

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.[11][12]

Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. [11][12]

CRYPTOGRAPHY TECHNIQUES AND KEY DISTRIBUTION METHODS

Cryptography is a technique to secure the data. It uses the concept of keys to change the form of input data, called encryption and data can be converted to previous form using the same keys, called decryption. [11]

TYPES OF CRYPTOGRAPHY

1. Public Key Cryptography: In this method, two different keys are used to secure the data. Public key is available to everyone and private key is kept secret. Sender can send the data to receiver by encrypting the data using his public key and receiver can decrypt the data using the its private key. [11]
2. Private Key Cryptography: In this method, a group of user share same key. Sender can send the encrypted data using private key and receiver can decrypt the data using same key. [12]

KEY DISTRIBUTION METHODS

1. Pre-distribution of keys: In this method, keys are assigned to each node for secure communication. Nodes can use these keys to share the data over network in a secure manner.
2. Post-distribution of keys: in this method, keys are assigned after the node deployment. Nod can obtained the keys from base station.[12]

SELECTION OF KEY DISTRIBUTION METHOD

Selection of cryptography method is a very critical issue for security implementation in WSNs. Many researchers consider that asymmetric key cryptography methods are not suitable for WSNs due to the resource limitation of sensor nodes. Although some recent research results show that it is feasible to apply asymmetric key cryptography to WSNs by choosing appropriate algorithms, parameters, etc., Key management is still too expensive in terms of computation and energy cost for sensor nodes, and still need further research. Symmetric key cryptography is more efficient then public key cryptography in terms of speed and low energy cost. However, the key management is not an easy task for symmetric key cryptography. There is need to developed more efficient and flexible key management scheme for WSN. [11]

2. LITERATURE SURVEY

Wireless sensor network is insecure by its nature: there is no such a clear line of defence because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviours that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the network. As a result, compared with the wired network, the wireless network will need more robust security scheme to ensure the security of it. [1][12]

Researchers have developed lot of different methods to secure the sensor network but each method has some sort of limitations. There are some critical operations like node authentication and key distribution. Now we will discuss the different schemes of authentication and key distribution used by the researchers.

J. Kim, J. Baek, T. Shon [1] suggested an efficient method of membership verification for re-authentication of mobile node and showed the performance analysis of membership verification. Using this method, they proposed an efficient and scalable re-authentication protocol over wireless sensor network. Also, they provided performance and security analysis of the protocol.

H. Wang and Y. Zhang [2] proposed an efficient threshold self-healing key distribution scheme with sponsorization for infrastructure less wireless networks. They claimed that the key distribution scheme satisfies the forward security, i.e., any internal user who has been revoked cannot generate a new session key. In this paper, an attack method against this key distribution scheme's forward security was presented. Furthermore, this attack method canalso be applied to this scheme's backward security. Thus, the original threshold self-healing key distribution scheme is insecure.

K. Han, T. Shon and K. Kim [3] extended novel and efficient node authentication and key exchange protocol that support Irregular distribution. Compared with previous protocols, this protocol has only a third of communication and computational overhead. The proposed improvement enables the efficient node re-authentication and key exchange even when the sensors are irregularly distributed to the smart home and WPAN for supporting various convergence services. In order to verify the proposed approach, they performed three kinds of validation according to communication pass, message size, and security analysis. From the analysis, improvement guarantees the longer lifetime of Smart Home Devices and WPAN while providing security solutions. In future work they will deploy the proposed approach to real Smart home environments and confirm the authentication operations for supporting NSL.

W. Wang and D. Peng [4] proposed a quality-driven scheme to optimize stream authentication and unequal error protection (UEP) jointly. This scheme can provide digital image authentication, image transmission quality optimization, and high energy efficiency for WMSN. The contribution of this research is two-fold as summarized below. First, a new resource allocation aware greedy stream authentication approach is proposed to simplify the authentication process. Second, an authentication-aware wireless network resource allocation scheme is developed to reduce image distortion and energy consumption in transmission. The scheme is studied by unequally protected image packets with the consideration of coding and authentication dependency.

They proposed a methodology for quality-driven and energy-efficient transmission of authenticated images in WMSNs. First, a JPEG2000 compatible stream authentication scheme is proposed with a minimal authentication dependency overhead, which is very easy to be integrated with network resource allocation schemes in order to tackle the problem of severe energy constraints in WMSNs. Furthermore, a general UEP-based network resource allocation framework is developed to optimize the image transmission quality with integrity and energy efficiency assurance. Simulation results demonstrate that the proposed schemes significantly improved the authenticated image quality even under strict communication energy consumption constraints in wireless multimedia sensor networks.

A. Rasheed and R. N. Mahapatra [5] proposed a general three-tier security framework for authentication and pair-wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Analysis indicates that with 10 per cent of the sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach. They have further improved the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes. They used the one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.

H. Dai and H. Xu [6] proposed a new key pre-distribution algorithm based on matrix-based technique and numerically evaluated. The proposed approach combines matrix-based method and polynomial-based key pre-distribution approach to achieve both high network connectivity and strong resilience against node capture. The effectiveness of the proposed algorithm has been demonstrated through analysis and simulation. Also, an efficient encoding mechanism was designed to optimize the memory overhead. In future work, they plan to develop the group-based matrix decomposition for the large distributed WSNs.

T. Kwon and J. Hong [7] proposed X-TESLA, an efficient scheme which may continue indefinitely and securely, that addresses this and many other issues of the previous schemes. With the advent of more powerful sensor node commodities such as iMote2, the future of public-key technique application to broadcast authentication looks bright, but X- TESLA can efficiently be combined with public-key techniques also. For example, they could modify X-TESLA to use digital signatures on Type 4 packets, keeping everything else the same. Through the application of TMD-trade off techniques they observed that care should be taken with the short-key-chain based broadcast authentication schemes.

Z. Liu, J. Ma Q. Huang, and Sang Jae Moon [8] presented an Asymmetric Key Pre-distribution Scheme. Instead of assuming that the network is comprised entirely of identical users in conventional key pre-distribution schemes, the network now consists of a mix of users with different missions, i.e., ordinary users and keying material servers. A group of users, using secret keys preloaded in their

properties of this method are that, the compromise of keying material servers does not reveal any information about users' secret keys and the session keys of privileged subset of users; if computational assumptions are considered, each user has very low storage requirement. These properties make it attractive for sensor networks. They first formally define the asymmetric key pre-distribution scheme in terms of the entropy and give lower bounds on user's storage requirement and the public keying material size. Then, they presented its constructions and applications for sensor networks.

P. F. Oliveira and J. Barros [9] considered the problem of secret key distribution in a sensor network with multiple scattered sensor nodes and a mobile device that can be used to bootstrap the network. Their main contribution is a set of secure protocols that rely on simple network coding operations to provide a robust and low-complexity solution for sharing secret keys among sensor nodes, including pairwise keys, cluster keys, key revocation, and mobile node authentication. Despite its role as a key enabler for this approach, the mobile node only has access to an encrypted version of the keys, providing information- theoretic security with respect to attacks focused on the mobile node. Results include performance evaluation in terms of security metrics and a detailed analysis of resource utilization. The basic scheme was implemented and tested in a real-life sensor network test bed. This class of network coding protocols to be particularly well suited for highly constrained dynamic systems such as wireless sensor networks.

K. Lu, Yi Qian, M. Guizani, and H. H. Chen [10] proposed a unified framework for distributed key management schemes in heterogeneous wireless sensor networks. Analytical models are developed to evaluate its performance in terms of connectivity, reliability, and resilience. Extensive simulation results show that, even with a small number of heterogeneous nodes, the performance of a wireless sensor network can be improvedsubstantially. It is also shown that these analytical models can be used to accurately predict the performance of wireless sensor networks under varying conditions.

3. PROBLEM FORMULATION

WIRELESS sensor networks are dense wireless networks of sensor nodes collecting and disseminating environmental data. Sensor nodes are small low-power devices constrained severely in their computation, communication, and storage capabilities, usually for economic reasons. They may sense around themselves, communicate over wireless channels within short ranges, and frequently fall into the sleep mode for saving their power. Accordingly, a large scale wireless sensor network is composed of a number of sensor nodes for covering wider area through multi-hop connections. It has various kinds of promising applications that include environmental monitoring. Since sensor nodes are deployed in unattended fashions or even in hostile environments, they can readily be captured and tampered by adversaries as well as communication links are compromised. [7]

To secure the communication over WSN there must be a authentication method which can ensure that unauthorized sensors cannot join the network as well as they cannot transmit the data over network.

Authentication issues for WSN

1. Authentication of Sensors

Sensor node can join the network at any time and can start communication over network but unauthorized node can join the network to access the data. So authentication of the nodes is essential. If nodes change their position dynamically then node re- authentication is required.

2. Authentication of Data

Sensors communicate with each other by sending the messages to each other. Each sensor should be able to verify the signature of the received message as well as the source of the message because attacker can also transmit the same messages.

3. Authentication of Key pair

It is very difficult to ensure that the keys which are being used in communication are the genuine keys. Intruder can also generate a key pair in order to replace the original one. After the replacement of keys, nodes may use the fake keys and the entire network can be compromised.

4. CONCLUSION

In this paper, we explored the different security issues of WSN, authentication and key distribution. Some authors talked about the various authentication schemes which can be used for node verification [1][2][4][5]. Some authors talked about the various key distribution schemes [6][7][8][9][10]. Research work done by these authors show that it is very challenging task to provide the secure communication over network and the need to discover more efficient methods with the respect of resource constraints of WSN.

Finally we can conclude that, to secure the communication over WSN there must be a provision to authenticate the data and as well as the sensors. It should also ensure that unauthorized sensors cannot join the network as well as they should not be able to transmit the data over network. Key management is also a very difficult task which can degrade the performance of entire network by consuming the resources for key computations.

REFERENCES

[1]Jangseong Kim, Joonsang Baek, Non-member, IEEE, Taeshik Shon, Member, IEEE," An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network", IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011

[2] Huaqun Wang and Yuqing Zhang, " Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10,NO. 1, JANUARY 2011

[3] Kyusuk Han, Taeshik Shon, Member, IEEE, and Kwangjo Kim, Member, IEEE," Efficient Mobile Sensor Authentication In Smart Home and WPAN", IEEE-2010

[4] Wei Wang, Member, IEEE, Dongming Peng, Member, IEEE, Honggang Wang, Member, IEEE, Hamid Sharif, Senior Member, IEEE, and Hsiao-Hwa Chen, Fellow, IEEE, "A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks With Stream Authentication", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 5,AUGUST 2010

[5] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks', IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012

[6] Hangyang Dai and Hongbing Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE SENSORS JOURNAL, VOL. 10, NO. 8, AUGUST 2010

[7] Taekyoung Kwon, Member, IEEE, and Jin Hong," Secure and Efficient Broadcast Authentication in Wireless Sensor Networks", IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 8, AUGUST 2010

[8] Zhihong Liu, Jianfeng Ma, Member, IEEE, Qiping Huang, and SangJae Moon, Member, IEEE," Asymmetric Key Pre-Distribution Scheme for Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009

[9] Paulo F. Oliveira, Student Member, IEEE, and João Barros, Member, IEEE," A Network Coding Approach to Secret Key Distribution", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 3, SEPTEMBER 2008

[10] Kejie Lu, Yi Qian, Mohsen Guizani, and Hsiao-Hwa Chen," A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 2, FEBRUARY 2008

[11] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009

[12] C Siva Ram Murthy, "Wireless Ad hoc Network-Architectures and Protocols", Pearson- 2012

Dynamics of Malware Spread in Decentralized Peer-to-peer Network

Tanmayi Mhatre, Dipali Shinde, Saili Budbadkar
Department Of Information Technology, P
admabhushan Vasantdada Patil Pratisthans College Of Engineering, Mumbai

ABSTRACT

Malware is the software developed with malicious intentions. The detection of such malware can be done by writing program which can understand the dynamics of malware. This paper presents an analytical model which can effectively characterize the true nature of malware and how it spreads in peer-to-peer networks such as Gnutella. The proposed model is compartmental model which involves derivation of network conditions and system parameters in such a way that under those parameters and conditions the underlying P2P network reaches a malware free equilibrium. The proposed model can also perform evaluation of strategies such as quarantine used to control malware spread. Afterwards the model has been enhanced and tested with networks of smart cell phones.

Keywords - Malware, Peer to Peer Decentralized Network.

1. INTRODUCTION

The use of peer-to-peer (P2P) networks as a vehicle to spread malware offers some important advantages over worms that spread by scanning for vulnerable hosts. This is primarily due to the methodology employed by the peers to search for content. For instance, in decentralized P2P architectures such as Gnutella where search is done by flooding the network, a peer forwards the query to its immediate neighbours and the process is repeated until a specified threshold time-to- live, TTL, is reached. Here TTL is the threshold representing the number of overlay links that a search query travels. A relevant example here is the Mandragore worm that affected Gnutella users.

The design of the search technique has the following implications: first, the worms can spread much faster, since they do not have to probe for susceptible hosts and second, the rate of failed connections is less. Thus, rapid proliferation of malware can pose a serious security threat to the functioning of P2P networks. Understanding the factors affecting the malware spread can help facilitate network designs that are resilient to attacks, ensuring protection of the networking infrastructure. This project addresses this issue and develops an analytic framework for modelling the spread of malware in P2P networks while accounting for the architectural, topological, and user related factors. We also model the impact of malware control strategies like node quarantine.

2. REVIEW OF LITERATURE

A. EXISTING SYSTEM:

Previous simulation model uses a combination of the Epidemiological model and a Empirical model to model the effect of large-scale worm attacks.

In an Existing system the complexity of the Empirical model makes it difficult to derive insightful results that could be used to contain the worm.

In a previous study it is used to detect the presence of a worm by detecting the trend, not the rate, of the observed illegitimate scan traffic.

The filter is used to separate worm traffic from background non worm scan traffic.

B. DISADVANTAGES OF EXISTING SYSTEM:

A. ASSUMPTIONS IN EPIDEMIOLOGICAL MODE

Epidemiological models to study malware spread in P2P networks. These studies assume that a vulnerable peer can be infected by any of the infected peers in the network. This assumption is invalid since the candidates for infecting a peer are limited to those within TTL hops away from it and not the entire network. Another important omission is the incorporation of user behavior. Typically, users in a P2P network alternate between two states: the on state, where they are connected to other peers and partake in network activities and the off state wherein they are disconnected from the network. Peers going offline result in fewer candidates for infection thereby lowering the intensity of malware spread.

B. EMPIRICAL MODEL IGNORES NODE DYNAMICS

An empirical model for malware spreading in BitTorrent is developed in while models for the number of infected nodes by dynamic hit list-based malware in BitTorrent networks is presented However, these models ignore node dynamics such as online-offline transitions and are applicable only to BitTorrent networks. the authors use hypercube as the graph model for P2P networks and derive a limiting condition on the spectral radius of the adjacency graph, for a virus/worm to be prevalent in the network. The models do not account for the fact that once a peer is infected, any susceptible peer within a TTL hop radius becomes a likely candidate for a virus attack.

C. PROPOSED SYSTEM:

Proposed model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage. We obtain the probability that the total number of hosts that the worm infects is below a certain level. Our strategy can effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advance or needing to explicitly detect the worm. Our automatic worm containment schemes effectively contain the worms and stop its spreading. In proposed system we are going to generate the graph containing information about both the active and inactive nodes. This node information will allow us to keep track of all nodes in TTL hops. Thus allowing us to identify infected nodes which are in active or inactive state.

D. COMPARISON WITH EXISTING SYSTEM:

1. Proposed system is more secured and accurate in comparison to existing system:-

The proposed system is more secure in comparison to existing system.It helps in better way to prevent and stop the attacks from the worms.The multiple scanning options helps the system to function in a better way.

2. Proposed system is less complex than the existing system:

The existing system uses a combination of the deterministic epidemic model and a general stochastic epidemic model to model the effect of large-scale worm attacks.In an Existing system the complexity of the general stochastic epidemic model makes it difficult to derive insightful results that could be used to contain the worm.The proposed model uses the automatic worm containment model.

3. Proposed system works more faster than the existing system:

The proposed model contains effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advanced or needing to explicitly detect the worm.

3. SYSTEM ARCHITECTURE:

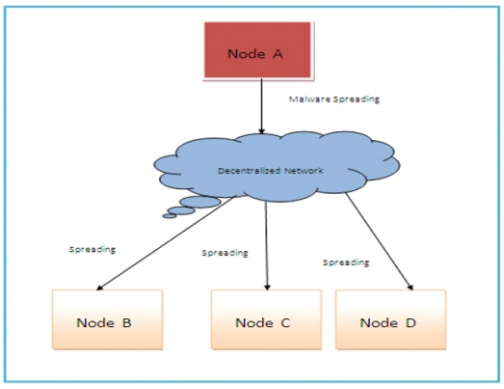

Figure .1:System Architecture

As Shown in the Figure1,

The architecture of DYNAMICS OF MALWARE SPREAD IN DECENTRALIZED PEER-TO-PEER NETWORK is based on decentralized peer to peer network The system consists of 5 main modules .The main modules are:

A. User Interface Design

In this module we have designed the user interface for all the hosts. We design the user interface to show our propagation of worms in a graphical manner or GUI. By showing the output in GUI gives more attractive and understandable to everyone. Then we design the containment window to show the scanning, detection of worms. Thus we design the whole user interface in this module.

B. Worm Propagation Model

In this module, we create a worm spreading model. This model is designed for the propagation of worms inside a network. Inside the network we spread the worms in a controlled environment. To create worm propagation model we need to form a network by using the server socket class and socket class available in Java. These two classes are used to create a connection to transfer data from a host to other host inside a network.

C. Scanning for worms

Our strategy is based on limiting the number of scans to dark-address space. The limiting value is determined by our analysis. Our automatic worm containment schemes effectively contain both uniform scanning worms and local preference scanning worms, and it is validated through simulations and real trace data to be non-intrusive.

D. Detecting and categorizing worms

The model is developed for uniform scanning worms and then extended to preference scanning worms. We detect these two worms and categorize it in this module.

E. Containment of worms

This model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, we are able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worm infects.

4. TECHNOLOGY AND CONCEPTS:

The following depicts the concepts and technology used in the proposed system.

A. AUTOMATIC WORM CONTAINMENT STRATERGY:

Automatic worm containment strategy prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, it is able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worm infects.

B. WORM TRAFFIC:

Worm Traffic is nothing but the traffic created due to the rapid proliferation and spreading of the worms on the network.Such network traffics may damage the functioning and thus may damage the overall system.

5. IMPLEMENTATION

For the development of the proposed system we have used Java and database whish is accomplished with Sql.

We have developed the GUI using java which are as follow:

Node A:

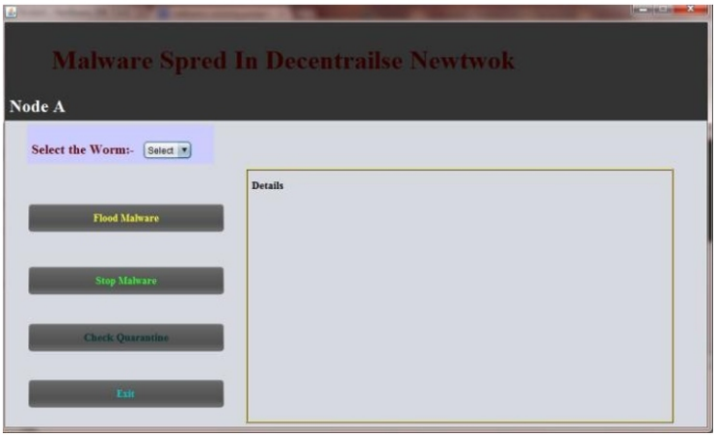

Fig.2 Node A

Node B:

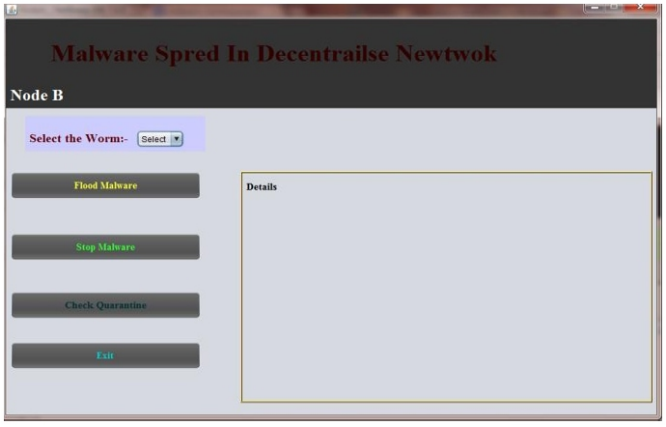

Fig.3 Node B

As shown in above GUI system will spread malware in network using „flood malware" option. The spread of malware can be controlled by using „stop malware" option on GUI. For detecting the malware during data transfer we have given the option „check quarantine" which will scan the packets coming to any node. And delete the contaminated packets.

The detailed information about data transfer can be seen in „details" window where the system will provide information about following:

1) Total packets transferred
2) Source node of received data
3) Total no. of contaminated packets
4) Total no. of packets discarded.

6. CONCLUSION

Dynamics of malware spread in decentralized peer to peer network is thus a system providing security for data transmission and communication in decentralized peer to peer network. It also provides security to devices in network against malware attack

.

The proposed system will provide the detailed information about states of devices in network, whether they are infected or not.

Proposed system will provide the status of data transfer in terms of total packets transferred, no. of infected packets and information about the node from which the infected data arrived at destination node.

Thus providing detailed information about nodes in network which will help for future data transfer in network.

ACKNOWLEDGEMENT

We are grateful to this institute for having channelized our skills and energy and for encouraging us to work together with cooperation and co-ordination. We are indebted to our inspiring HEAD OF DEPARTMENT and Internal Project Guide MRS.PRACHI KSHIRSAGAR and also our Principal Dr.K.T.V REDDY who have extended all valuable guidance, help and constant encouragement through the various difficult stages in the development of the project.

REFERENCES

[1] Krishna ,Ramachandran and BiplabSikdar,"Dynamics of Malware Spread in Decentralized Peer-to-Peer Networks", IEEE Transactions on Dependable and Secure Computing, Vol. 8, No.4, July/August 2011.

[2] Andrew Kalafut, Abhinav Acharya, Minaxi Gupta, "A Study of Malware in Peer-to-peer Networks".

[3] "Anticipation Measures For Protecting P2P Networks From Malware Spread", The International Journal of Engineering And Science(Ijes) Vol.2, Issue-2,2013

[4] BOOK: Complete Reference JAVA.

[5] X. Yang and G. de Veciana, "Service Capacity in Peer-to-Peer Networks," Proc. IEEE INFOCOM "04, pp. 1-11, Mar. 2004.

[6] J. Mundinger, R. Weber, and G. Weiss, "Optimal Scheduling of Peer-to-PeerFile Dissemination," J. Scheduling, vol. 11, pp. 105-120, 2007.

[7] A. Bose and K. Shin, "On Capturing Malware Dynamics in Mobile Power-Law Networks," Proc. ACM Int"l Conf. Security and Privacy in Comm.Networks (SecureComm), pp. 1-10, Sept. 2008.

[8] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien, "AFirst Look at Peer-to-Peer Worms: Threats and Defenses," Int"l WorkshopPeer-To-Peer Systems, Feb. 2005.

[9] F. Wang, Y. Dong, J. Song, and J. Gu, "On the Performance of PassiveWorms over Unstructured P2P Networks," Proc. Int"l Conf. IntelligentNetworks and Intelligent Systems (ICINIS), pp. 164-167, Nov. 2009.

[10] R. Thommes and M. Coates, "Epidemiological Models of Peer-to-PeerViruses and Pollution," Proc. IEEE INFOCOM "06, Apr. 2006.

Survey Of Flooding Attack in Mobile Adhoc Network

Guide – Mr.neeraj shukla,
Mansi kharya
Gyan ganga college of technology

ABSTRACT

Mobile ad hoc networks will appear in environments where the nodes of the networks are absent and have little or no physical protection against tampering. The wireless nodes of MANET are thus susceptible to compromise and are particularly vulnerable to denial of service (DoS) attacks launched by malicious nodes or intruders. Flooding attack is one such type of DoS attack, in which a compromised node floods the entire network by sending a large number of fake RREQs to nonexistent nodes in the network, thus resulting in network congestion. In this paper, the security of MANET AODV routing protocol is investigated by identifying the impact of flooding attack on it. A simulation study of the effects of flooding attack on the performance of the AODV routing protocolis presented using random waypoint mobility model The simulation environment is implemented by using the NS-3 network simulator. It is observed that due to the presence of such malicious nodes, average percentage of packet loss in the network, average routing overhead and average bandwidth requirement− all increases, thus degrading the performance of MANET significantly.

Keywords - AODV; flooding attack; malicious nodes; MANET; NS-3 simulation; packet loss; wireless security

1. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a group of wireless mobile hosts, which has no stationary infrastructure or base station for communication. Each individual node communicates beyond their direct wireless transmission range by cooperating with each other and forwarding packets through multi-hop links. The nodes act as routers for forwarding and receiving packets to/from other nodes. Ad hoc networking are extensively use for military purposes, disaster relief, mine site operation, etc. For such applications, a secure and reliable communication is necessary. Routing in ad hoc networks [2] [3] [4] has been a challenging task ever since wireless networks came into existence. Due to the high mobility of nodes, interference, multipath propagation and path loss, there is no fixed topology in MANET. Hence a dynamic routing protocol is needed for these networks to function properly.

Dynamic routing protocols can be classified as proactive and reactive routing protocols, as follows:

The proactive (table-driven) routing protocols like DSDV [5], etc. maintain the routing information to every other node in the network, even before it is needed.

The reactive (on-demand) routing protocols like AODV [6], DSR [7] etc., do not maintain the routing informations to other nodes in the network, until and unless required. This type of protocols finds a route on demand by flooding the network with Route Request packets.

In many situations, the on-demand (reactive) routing protocols have proved to perform better with significantly lower overheads than the periodic (proactive) routing protocols. This is because the on-demand protocols can react quickly to the dynamically changing topology, while reducing the routing overhead in those areas of the network, where changes are less frequent. In this paper, the focus is mainly on the reactive routing protocols (namely AODV) for MANET. unsuitable.

All available nodes in ad hoc networks participate in routing and forwarding, in order to maximize the total network throughput. Hence, successful operation of MANET is possible if and only if all the participating nodes fully cooperate in communication. Due to the lack of afixed base station, the ad hoc nodes are forced to rely on each other to maintain network stability and functionality. However, misbehaving nodes [8] [9] [10] are capable of causing significant problems. A node may misbehave when it is overloaded, broken, selfish, or malicious.

A malicious node [11], also called compromised node, can sabotage the other nodes or even the whole network, by launching a denial of service attack, by either dropping packets or by flooding the network with a large number of RREQs to invalid destinations in the network, thus jamming the routes of communication. Flooding attack is one such type of DoS attack, in which a compromised node floods the entire network by sending a large number of fake RREQs to nonexistent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network. This results in network congestion, thus leading to a Denial of Service.

In this paper, a simulation study of impact of flooding attack in AODV [6] performance, using the NS-3 network simulator is given.

The rest of the paper is organized as follows. In section II, an overview of the AODV routing protocol is presented, followed by a briefing about the NS-3 network simulator in section III. The impact of flooding attack in MANET is discussed in section IV. In section V, the simulation parameters used are given, followed by the simulation results in section VI and concluding remarks in section VII.

II. OVERVIEW OF THE AODV PROTOCOL

The Ad hoc On-demand Distance Vector (AODV) [6] routing protocol is a simple and efficient on-demand routing protocol, based on the distance vector approach. It is designed specifically for use in multi-hop wireless MANET scenario. The protocol is composed of the two main mechanisms − "Route Discovery" and "Route Maintenance".

Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of routing table entries. Route Request (RREQ) message is broadcasted by a node requiring a route to another node and Route Reply (RREP) message is unicasted back to the source of RREQ. Sequence numbers are used for each routing table entry to determine whether the routing information is up-to-date. This prevents routing loops.

AODV includes the route maintenance mechanism to handle the dynamic network topology. Routes are maintained by using Route Error (RERR) message, which is sent to notify other nodes about a link failure. HELLO messages are sent in periodic beacons for detecting and monitoring the links to the neighbors.

If a node S wants to send data packets to a destination D that is not in its routing table, it will buffer the data packets and broadcast a Route Request (RREQ) for D into the network. The RREQ packet will be forwarded by other intermediate AODV nodes to the intended destination node D. On receiving the RREQ, D will send a Route Reply (RREP) on the reverse route back to S. S includes the known sequence number of the destination in the RREQ packet. The intermediate nodes, on receiving an RREQ packet check its routing table entries. If it possesses a fresh route toward D, i.e. a route with greater sequence number than that in the RREQ packet, it unicast an RREP packet back to its neighbor from which it has received the RREQ packet. Otherwise, it sets up the reverse path and then rebroadcasts the RREQ packet. Duplicate RREQ packets received by one node are silently dropped. As the RREP packet is propagated along the reverse path to the source, the intermediate nodes update their routing tables and set up the forward path.

III. THE NS-3 SIMULATOR

For simulation analysis, NS-3 [12] [13] was used for implementing the network simulation environment. NS-3 is an open source discrete event network simulator targeted primarily for networking research and educational purpose. Previously, NS-2 [14] was the tool for academic networking research. But it had several disadvantages. It required the involvement of both oTcl and C++. For new modules and features, it required a lot of manual recoding and compilations.

NS-3 is a new simulator. It is not an extension of NS-2. It does not support the NS-2 APIs. It is written entirely in C++, with optional Python bindings. Hence, simulation scripts can be written either in C++ or in Python. The oTcl scripts are no longer needed for controlling the simulation, thus abandoning the . problems which were introduced by the combination of C++ and oTcl in NS-2. Thus, NS-3 is a more readily extensible platform and much easier to use.

NS-3 has sophisticated simulation features, which include extensive parameterization system and configurable embedded tracing system, with standard outputs to text logs or PCAP (tcpdump). It is very object oriented for rapid coding and extension. It has an automatic memory management capability as well as an efficient object aggregation/query for new behaviors & states, like adding mobility models to nodes. Moreover, NS-3 has new capabilities, such as handling multiple interfaces on nodes correctly, efficient use of IP addressing and more alignment with Internet protocols and designs and more detailed 802.11 models, etc. NS-3 integrates the architectural concepts and code from GTNetS [15], which is a simulator with good scalability characteristics. The Simulation Network Architecture looks just like IP architecture stack. The nodes in NS-3 may or may not have mobility. The nodes have "network devices", which transfer packets over channel and incorporates Layer 1 (Physical Layer) & Layer 2 (Data Link layer). The network devices acts as an interface with Layer 3 (Network Layer: IP, ARP). The Layer 3 supports the Layer 4 (Transport Layer: UDP, TCP), which is used by the Layer 5 (Application Layer) objects.

IV. IMPACT OF FLOODING ATTACK

A malicious (compromised) node generally aims to launch a denial of service in the whole network. Flooding attack [11] [16] [17] [18] is a denial of service attack, in which a compromised node floods the network by sending large number of fake RREQs to nonexistent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network.

Flooding attack can be classified into two types [17]: RREQ Flooding Attack and Data Flooding Attack

A. RREQ Flooding Attack

The RREQ Flooding Attack is a denial-of-service attack in which malicious nodes take advantage of the route discovery process of the reactive routing protocols (e.g. AODV, DSR) in MANET. In this attack, a compromised node aims to flood the network with a large number of RREQs to non-existent destinations in the network. It generates a large number of RREQs and broadcast them to invalid destinations. Since a node with such invalid destination node-id does not exist in the network, a reply

When such fake RREQ packets are broadcasted into the network in high numbers, the network gets saturated with RREQs and is unable to transmit data packets. Thus, it leads to congestion in the network. The RREQ Flooding Attack also results in overflow of route table in the intermediate nodes sothat the nodes cannot receive new RREQ packet, resulting in a denial- of-service attack. Moreover, unnecessarily forwarding these fake route request packets cause wastage of precious node resources such as energy and bandwidth.

To reduce congestion in a network, the AODV protocol adopts some methods. RREQ_RATELIMIT [19] is the maximum allowable number of RREQs that a node can sent per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may again try to discover a route by broadcasting another RREQ, until the numbers of retries reach the maximum TTL value. The default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. However, a malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node can do so because of its self-control over its parameters. This allows it to flood the network with fake route requests, leading to a kind of DoS attack due to the network-load imposed by the fake RREQs.

B. Data Flooding Attack

Once an attacker node has set up the paths to all the nodes in the networks, it may cause DATA Flooding Attack by streaming large volumes of useless DATA packets to them along these paths. The excessive DATA packets in network clog the network and reduce the available network bandwidth for communication among the other nodes in the network. Thedestination node gets busy on receiving the excessive packets from the attacker and cannot work normally. The available network bandwidth for communication also gets exhausted, so that the other nodes cannot communicate with each other due to the congestion in the network. Moreover, the process of receiving the attack packets consumes a lot of resource in all the intermediate nodes.

If an attacker combines both types of flooding attacks, it will result in the whole network crashing.

Due to flooding attack, a non-malicious genuine node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs and useless data packets. This leads to several problems, as follows:

- Wastage of bandwidth

- Wastage of nodes' processing time, thus increasing the overhead
- Overflow of the routing table entries, causing exhaustion of an important network resource like memory
- Exhaustion of the nodes' battery power
- Degraded throughput

Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication.

V. SIMULATION SETUP

The simulation was done using the NS-3 simulator [12], which provides a scalable simulation environment for wireless networks. In order to measure the impact of flooding attack in MANET performances, the AODV routing protocol was modified to simulate a flooding attack scenario.

The simulated network consists of 16 nodes placed randomly in 500x500 areas. For different scenarios of simulation, Constant position mobility and Random-walk 2D mobility model are used. Each node moves at a speed of 20 m/s.

The Ping application was used in the application layer. To simulate flooding attack, some malicious nodes were introduced to flood the network. These flooding nodes generated fake RREQ packets with invalid destination addresses and broadcasted them in the network at the rate of 8 packets per sec. By default, RREQ_RATELIMIT [19] of each node is 10, as proposed by RFC 3561. This RREQ_RATELIMIT was changed to 50.

The simulation parameters along with their values are listed down in Table I.

TABLE I. SIMULATION PARAMETERS

Parameters	Values
routing protocol	AODV
simulation time	60s
number of mobile	95
transmission area	1000 x1000
mobility model	Random-walk 2d
traffic type	UDP
data packet size	1024Bytes
rate	2Kbps
speed of node	20m/s
RREQ_RATELIMIT	50

VI. SIMULATION RESULTS

After simulating the flooding attack in AODV, some graphs were plotted and they were used to see the simulation results when the network gets flooded by fake RREQs to invalid destinations.

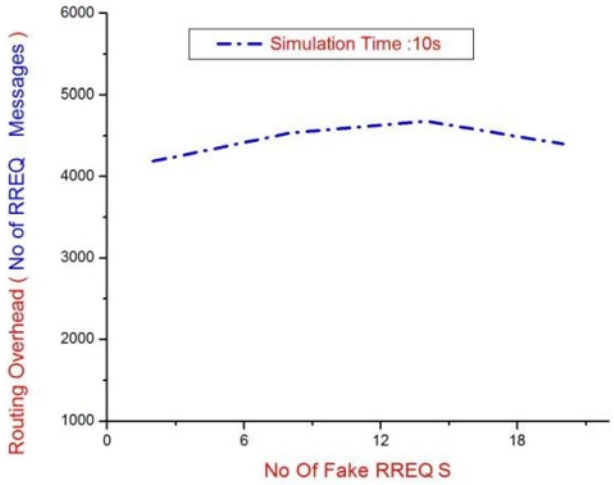

Figure 1. Number of Fake RREQs vs. Routing Overhead

For the simulation in Fig. 1, fake RREQ packets were generated and the total number of original RREQs that arrived at each node was calculated. Routing Overhead denotes the total number of RREQ messages (original, as well as fake) broadcasted in the network. The graph in Fig. 1 depicts that the average Routing Overhead increases with the number of fake RREQs. Because of these fake RREQ messages, routing table of each node needs to maintain more entries, thus creating an extra overhead.

For Fig. 2 simulation, the total number of data packets that were dropped due to the RREQ flooding was calculated. The graph depicts that the average percentage of data packet loss increases with the increase

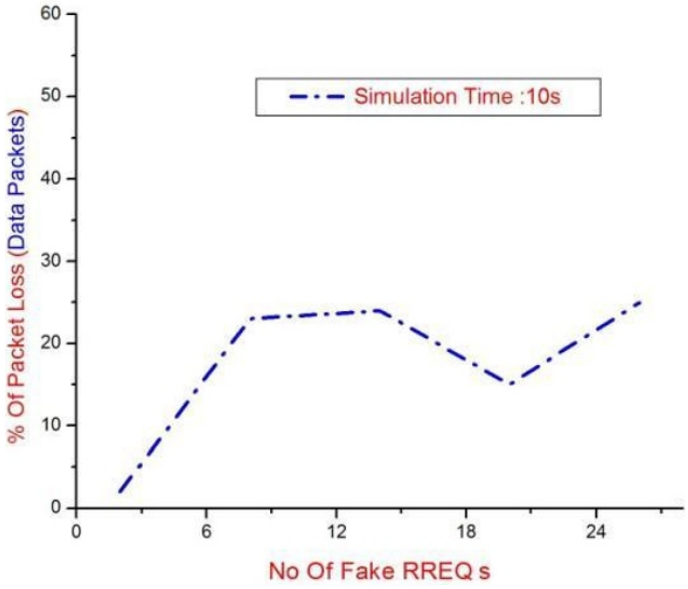

Figure 2. Number of Fake RREQs vs. Percentage of Data Packet Loss

Next, some flooding nodes were introduced, which generate eight RREQs per second. The graph in Fig. 3 depicts that with the increase in the number of flooding nodes, Routing Overhead, (i.e. total number of original and fake RREQ packets in the network) increased drastically.

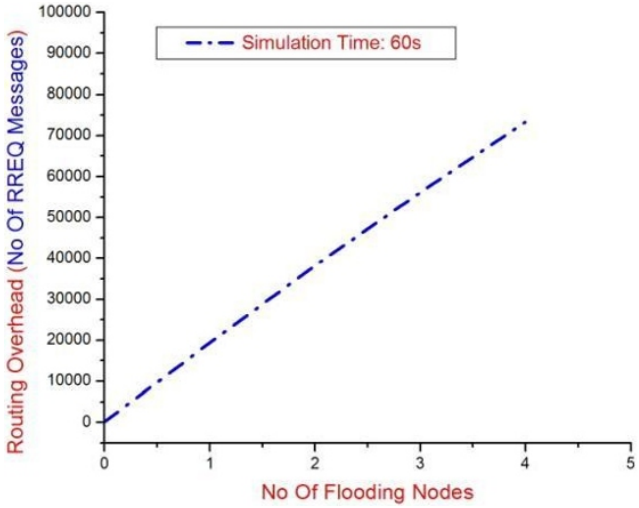

Figure 3. Number of Flooding Nodes vs. Routing Overhead

The bandwidth usage in the network was calculated, as follows:

Bandwidth usage =

(Total num of packets received/Simulation Time)*(8/1000) Bandwidth usage of a network is inversely proportional to the throughput of the network.

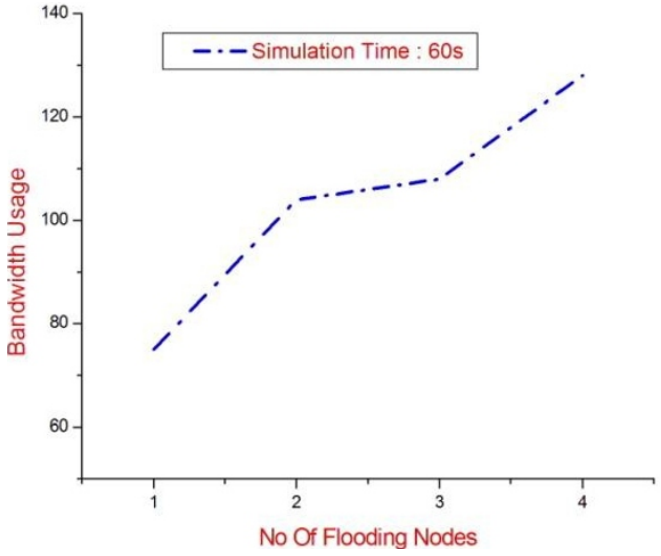

Figure 4. Number of Flooding Nodes vs. Bandwidth Usage

The graph in Fig. 4 depicts that the average bandwidth usage of the network increases as more flooding nodes join the network. Because of this flooding attack, average bandwidth usage of the network increases considerably, thus decreasing the network throughput.

Fig. 5 shows the average percentage of data packet loss due to the presence of flooding nodes in the network. The graph depicts that the average percentage of data packet loss in the network increases with the number of flooding nodes.

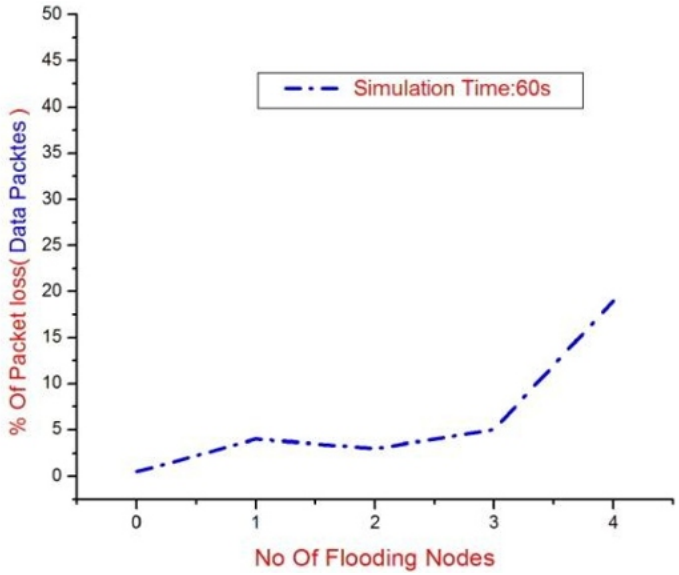

Figure 5. Number of Flooding Nodes vs. Percentage of Data Packet Loss

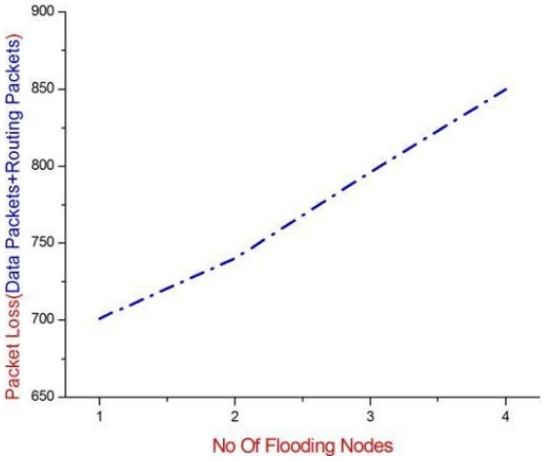

Figure 6. Number of Flooding Nodes vs. Percentage of Overall Packet Loss (Data and Routing Packets)

Due to the flooding attack, the network gets congested, resulting in a loss of RREQ packets as well. The graph in Fig. 6 depicts that as the number of flooding nodes in the network increases, the average packet loss (both data and routing packets) also increases in the network.

VII. CONCLUSION

In this paper, the security of AODV routing protocol in MANET was investigated by identifying the impact of flooding attack on it. The flooding attack in AODV protocol was simulated using the NS-3 network simulator. However, similar results can also be found when using the DSR [7] routing protocol. It was noticed that the presence of malicious flooding nodes in MANET can affect the performance of the overall wireless network and can act as one of the major security threats. From the simulation, it can be concluded that due to the extensive flooding in the network, average percentage of packet loss, average routing overhead and average bandwidth requirement– all increases, thus decreasing the overall network throughput.

A strong monitoring mechanism must be implemented in the mobile nodes of MANET for the identification and isolation of the compromised flooding nodes from the network. Some sort of incentive mechanism may also be incorporated in the network to enforce cooperation among all the nodes in MANET to improve the overall network performance.

In future work, a reputation based trust mechanism is proposed, which helps to resist misbehavior in the network by motivating the nodes to enhance cooperation and thus improve the network performance.

REFERENCES

[1] S Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". Internet Request for comment RFC 2501, Jan 1999.

[2] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks". Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

[3] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, "Routing security in ad hoc wireless networks", Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[4] Krishna Gorantala, "Routing Protocols in Mobile Ad-hoc Networks".June 15, 2006 Master's Thesis in Computing Science, 10 credits; Supervisor at CS- UmU: Thomas Nilsson; Examiner: Per Lindstrom.

[5] C. Perkins and P Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers". In ACM SIGCOMM'94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234 -244.

[6] C.E. Perkins, E. Belding Royer, and S.R. Das, "Ad hoc On demand distance vector (AODV) routing", IETF RFC 3561, July 2003.

[7] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728,2007.

[8] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks". International Conference on Mobile Computing and Networking, Proceedings of the 6th annua international conference on Mobile computing and networking, 2000, Boston, Massachusetts, United States, pgs. 255 – 265.

[9] A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols". IETF RFC4593. Status Informational, October, 2006.

[10] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer, 2008.

[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routingattacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[12] "The NS-3 Network Simulator", http://www.nsnam.org/

[13] Elias Weingartner, Hendrik vom Lehn, Klaus Wehrle, "A performance comparison of recent network simulators". In Proceedings of the IEEE International Conference on Communications 2009 (ICC 2009), Dresden, Germany, 2009.

[14] "The NS-2 Network Simulator", http://www.isi.edu/nsnam/ns

[15] G. Riley, "Large scale network simulations with GTNetS", in Proceedings of the 2003 Winter Simulation Conference, 2003.

[16] S. Sanyal, A. Abraham, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N. Mody, "Security scheme for distributed DoS in mobile ad hoc networks", 6th International Workshop on Distributed Computing (IWDC'04), vol. 3326, LNCS, Springer, 2004, pp. 541.

[17] P. Yi, Z. Dai, Y. Zhong, S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), April 2005, pp. 657-662.

[18] Z. Eu and W. Seah, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan, January 2006.

*[19] Perkins C.E., T*erminology for Ad-Hoc Networking, Draft-IETF- MANETterms- 00.txt, November 1997.

Demographic Perception Towards Mobile Banking in India

Sultan Singh[1], Madhu Arora[2]
[1]Professor, Department of Business Administration, Chaudhary Devi Lal University, Sirsa -125055
[2]Research Scholar, Department of Commerce, Chaudhary Devi Lal University, Sirsa - 125055

ABSTRACT

The present study is conducted to know the demographic perception toward mobile banking in selected public, private and foreign banks. A sample of 187 respondents was selected on the basis of judgement sampling from the banks which are providing mobile banking facility to the customers from Delhi and NCR. To find out the patterns of relationship that exist among data- groups, statistical tools used for this purpose are Standard Deviation, Regression Analysis, t- test, Z-test. The results show that age has significant impact on agreement on boost up of security risk solutions. There is a significant difference in the average agreement on boost up of security risk solutions, performance/service quality risk solutions, technological risk solutions and financial risk solutions in mobile banking of unmarried and married respondents. However, unmarried respondents consider security risk solutions, performance/service quality risk solutions, technological risk solutions and financial risk solutions most important than married respondents to boost up the mobile banking. There is no significant difference in the average agreement on problems in mobile banking amongst the different education levels. It is recommended that SMS (short message service) and push messages for smart phones, customer authentication such as Personal Identification Numbers (PIN), review of privacy protection policies, providing information to the customers on the importance of safeguarding information in non-secure transactions are necessary to boost up the mobile banking amongst the customers. Customers should also be advised to have unbreakable passwords for the protection of their transactions.

Keywords - Demographic, Personal Identification Numbers, Privacy, Non-secure Transactions.

1. INTRODUCTION

Mobile phones, as a medium for extending banking services, have of-late attained greater significance because of their ever-present nature. „Mobile Banking transaction" means undertaking banking transactions using mobile phones by bank customers that involve accessing/ credit/ debit to their accounts. Banks are permitted to offer mobile banking services after obtaining necessary permission from the Department of Payment & Settlement Systems and Reserve Bank of Delhi and NCR. The rapid growth of mobile banking customers in Delhi and NCR, through wider coverage of mobile phone networks, have made this medium an important platform for extending banking services to every segment of banking clientele in general and the unbanked segment in particular.

REVIEW OF LITERATURE

Various articles on varied aspects of mobile banking appeared in different journals, but they are restrictive in nature and do not give a comprehensive nature. **Supathanish** (2010) investigated the level of satisfaction and trust in using MB in Northern Region of Thailand and tried to find out the reasons for not using MB. It was observed that the service quality, perceived risk factors, user input factors, employment and education were the dominant variables that influence consumers' choice of electronic banking and non-electronic banking channels. **Anani** (2010) examined the banking industry‟s ways of attracting and retaining customers leading to customer satisfaction which in turn lead to increased profitability. The results of the show that customers have concerns with regard to the banks they conduct business with. The respondents were generally satisfied to some extent with their banks with regard to services, products and banking relationship. It was suggested that the banks need to do research on why customer satisfaction is low. **Vaidya** (2011) examined the emerging trends on functional utilization of mobile banking in developed markets in next 3-4 years, for achieving objectives of getting information about banking organizations such as customer communication and information, customer convenience, conduct transactions, create customer centricity, enrich mobile banking experience to non- banking financial services, building the customer relationship, extract the best advantage of technology, provide value-added propositions, generate new revenue stream, reduce cost of transactions, achieve multi-channel advantage, automate the servicing and support research methodology was based on all secondary data by analyzing different literature on the topic. It was suggested that less developed market could adopt mobile based transactions irrespective of the type of handset due to innovative products especially in “fund transfer” or “remittances” segment with collaboration between telecom companies, payment providers, banks, etc. and some of the selected features have been effectively utilized in these markets. However, the high- featured mobile phones in smart environment would definitely take mobile banking to the next level in the next 3 to 4 years from now. **Malarvizhi** & **Rajeswari** (2012) examined the awareness and usage of mobile banking services and estimated the criteria for selecting the mobile banking services in Coimbatore city and found that mobile banking users were mostly educated, belonged to business group and middle income group. Customers perceived the mobile banking more useful but the banks must be ready to meet their expectations and provide them a hassle-free mobile banking experience. **Lalitha** (2014) tried to know the latest innovations introduced in commercial and private banks, and analyzed the adoption practices of customers regarding innovative banking product and customer satisfaction towards these innovative banking products. It was found that customers choose banks on the basis of location and accessibility. Many of the respondents were not using these innovative products either due to lack of knowledge or inaccessibility to the products. Many of the respondents were observed as beginners in the usage of computers. ATM card was found to be the most opted innovative product rather than internet banking

and mobile banking. Customers were found suffering from technophobia which was observed as a hindrance in usage of internet banking and mobile banking due to increased rate of frauds. As a result, respondents were found hesitating in the adoption of innovative products.

SCOPE OF THE STUDY

The present study has been conducted to know the demographic perception towards mobile banking in selected public, private and foreign banks in Delhi and NCR.

OBJECTIVES OF THE STUDY

The main objective of the study is to examine the perception towards mobile banking in the selected banks. In this broader framework, the following are the specific objectives of the study:

(I) To study the relationship of variables with the use of mobile banking of the demographic in the selected banks.

(ii) To examine the impact of mobile banking on customer satisfaction by analyzing the problems faced by the demographic in the selected banks.

(iii) To suggest measures to boost up the services in mobile banking for the betterment of the society.

RESEARCH METHODOLOGY

Sample Design

The universe for the purpose of this study comprises of all the banks in Delhi and NCR. For the present study, judgmental sampling is used for selection of 187 customers using mobile banking. Sample has been taken from those selected banks which are providing mobile banking facility to the customers from Delhi and NCR.

Data Collection

The present study includes both primary and secondary data. Primary data have been collected from the customers with the help of pre-structured questionnaire and secondary data have been extracted from the Annual Reports of the selected banks, national and international agencies, various RBI Publications and IBA Publications, etc. The other sources include the research studies and articles published in various journals, magazines, newspapers and websites.

Data Analysis

To find out the patterns of relationship that exists among data-groups, statistical tools used are Standard Deviation, Regression analysis, t-test, Z-test and Chi-square test. Data have been analyzed with the help of Statistical Package of Social Science (SPSS).

RESULTS AND DISCUSSIONS

Correlation of Age with different Variables

Firstly, it has been found out whether age is associated with average Agreement on problems in mobile banking (X1), average agreement on customer satisfaction (X2), average infrastructure risk (X3), average political and regulatory risk (X4), average service quality risk (X5), average personalized risk (X6), average security risk (X7), average operational/technological risk (X8),average agreement on boost up of security risk solutions (X9), average agreement on boost up of technological risk solutions (X10), average agreement on boost up of financial risk solutions (X11), average agreement on boost up of performance/service quality risk solutions (X12). From the results of correlation analysis, it is clear that age has significant impact only on average agreement on boost up of security risk solutions as p value is less than 0.10 at 10 percent level of significance.

Table 1: Correlation among Age and Problems in Mobile Banking

Y	Name	Y	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}
Age (Yrs)	R	1	-0.11	-0.11	-0.04	-0.05	-0.05	0.04	-0.04	-0.05	0.13*	0.1	0.11	0.12
	P		0.12	0.11	0.61	0.46	0.48	0.64	0.63	0.52	0.09	0.18	0.15	0.11
	N	-	187	187	187	187	187	187	187	187	187	187	187	187
*. Significant at the 0.10 level (2-tailed)														

Source: Survey

Marital Status and Perception about solutions to different Risks in Mobile Banking

In this section, an attempt is made to analyze the relationship between marital status and perceptions of the customers about the solutions to different risks in mobile banking. Table 2 and 2.1 shows that there is a significant difference in the average agreement on boost up of security risk solutions in mobile banking of unmarried (Mean = 3.60, SD = 0.88) and married respondents (Mean = 3.20, SD = 0.94), t = 3.04, p=0.003. However, unmarried respondents consider security risk solutions most important than married to boost up mobile banking.

Table 2: Group Statistics for Security Risk Solutions in Mobile Banking

	Marital Status	N	Mean	Std. Deviation	Std. Error of Mean
Average Agreement on Boost up of Security Risk Solutions	Unmarried	93	3.6	0.88	0.09
	Married	94	3.2	0.94	0.09

Source: Survey

Table 2.1 Independent Samples Test

		F	p	T	d.f.	p	Mean Diff.	Std. Error	95% Confidence Interval of the Difference	
									Lower	Upper
(A)	Equal σ assumed	2.6	0.11	3.04	185	0.003	0.41	0.13	0.14	0.67
	Not Equal σ assumed			3.04	184	0.003	0.41	0.13	0.14	0.67

Source: Survey

Table 3 and 3.1 shows that there is a significant difference in the average agreement on boost up of technological risk solutions in mobile banking of unmarried (Mean = 3.69, SD = 0.91) and married respondents (Mean = 3.24, SD = 0.96), t = 3.30, p=0.001. However, unmarried respondents consider technological risk solutions most important than married to boost up mobile banking.

Table 3: Group Statistics for Technological Risk Solutions in Mobile Banking

	Marital Status	N	Mean	Std. Deviation	Std. Error of Mean
Average Agreement on Boost up of Technological Risk Solutions	Unmarried	93	3.69	0.91	0.09
	Married	94	3.24	0.96	0.09

Source: Survey

Table 3.1: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equalit Meansy of						
		F	p	t	d.f.	p	Mean Difference	Std. Error	95% Confidence Interval of the Difference	
									Lower	Upper
(B)	Equal σ assumed	4.03	0.045	3.30	185	0.01	0.45	0.14	0.18	0.72
	Equal σ not assumed			3.29	184	0.01	0.45	0.14	0.18	0.72

Source: Survey

Table 4 and 4.1 shows that there is a significant difference in the average agreement on boost up of financial risk solutions in mobile banking of unmarried (Mean = 3.70, SD = 0.85) and married respondents (Mean = 3.32, SD = 0.93), t = 2.95, p=0.004. However, unmarried respondents consider financial risk solutions most important than married to boost up the mobile banking.

Table 4: Group Statistics for Financial Risk Solutions in Mobile Banking

	Marital Status	N	Mean	Std. Deviation	Std. Error of Mean
Average Agreement on Boost up of Financial Risk Solutions	Unmarried	93	3.7	0.84	0.088
	Married	94	3.32	0.93	0.096

Table 4.1: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	p	t	d.f.	p	Mean Difference	Std. Error	95% Confidence Interval of the Difference	
									Lower	Upper
(C)	Equal σ assumed	2.94	0.088	2.95	185	0.01	0.38	0.13	0.13	0.64
	Equal σ not assumed			2.95	183	0.01	0.38	0.13	0.13	0.64

Source: Survey

Table 5 and 5.1 shows that there is a significant difference in the average agreement on boost up of performance/service quality risk solutions in mobile banking of unmarried (Mean = 3.75, SD= 0.86) and married respondents (Mean = 3.38, SD = 0.96), t = 2.78, p=0.006. However, unmarried respondents consider performance/service quality risk solutions most important than married to boost up the mobile banking.

Table 5: Group Statistics for Service Quality Risk Solutions in Mobile Banking

	Marital Status	N	Mean	Std. Deviation	Std. Error of Mean
Average Agreement on Boost up of Performance/Service Quality Risk Solutions	Unmarried	93	3.75	0.86	0.09
	Married	94	3.38	0.96	0.09

Source: Survey

Table 5.1: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	p	T	d.f.	p	Mean Difference	Std. Error	95% Confidence Interval of the Difference	
									Lower	Upper
(D)	Equal variances assumed	3.01	0.085	2.78	185	0.01	0.37	0.13	0.11	0.64
	Equal variances not assumed			2.78	183	0.01	0.37	0.13	0.11	0.64

Source: Survey

Education Levels and Perceptions about Problems in Mobile Banking

Table 6 and 6.1 shows the relationship between education level and perception of the customers about the solutions to different risks in mobile banking. From the results, it is clear that there is no significant difference in the average agreement on problems in mobile banking amongst the different education levels $\{F(3, 183) = 1.15, p = 0.33\}$.

Table 6: Descriptive on Average Agreement on Problems in Mobile Banking at different Education Levels

	N	Mean	S.D.	Std. Error	95% Confidence level		Min.	Max.
					Lower Bound	Upper Bound		
U.G.	79	2.85	0.68	0.08	2.69	2.99	1.18	4.32
Graduate	51	2.68	0.76	0.11	2.46	2.89	1.14	4.09
P. G.	33	2.81	0.78	0.14	2.54	3.09	1.68	4.32
PhD	24	2.58	0.74	0.15	2.26	2.89	1.18	3.95
Total	187	2.76	0.73	0.05	2.65	2.87	1.14	4.32

Source: Survey

Table 6.1: Analysis of Variance

	Sum of Squares	d.f.	Mean Square	F	p
Between Groups	1.84	3	0.614	1.15	0.33
Within Groups	97.54	183	0.533		
Total	99.38	186			

Source: Survey

CONCLUSION AND POLICY IMPLICATIONS

To sum up, age has significant impact on agreement on boost up of security risk solutions. There is a significant difference in the average agreement on boost up of security risk solutions, performance/service quality risk solutions, technological risk solutions and financial risk solutions in mobile banking of unmarried and married respondents. However, unmarried respondents consider security risk solutions, performance/service quality risk solutions, technological risk solutions and financial risk solutions most important than married respondents to boost up mobile banking. There is no significant difference in the average agreement on problems in mobile banking amongst the different education levels. It is recommended that SMS (short message service) and push messages for smart phones, customer authentication such as Personal Identification Numbers (PIN), review of privacy protection policies, providing information to the customers on the importance of safeguarding information in non-secure transactions are necessary to boost up the mobile banking amongst the customers. Customers should also be advised to have unbreakable passwords for the protection of their transactions. Use of facial recognition technology may be a milestone to boost up the mobile banking amongst the customers.

REFERENCES

- *Supathanish Termsnguanwong (2010), "Customers' Discernment of Mobile Banking Business: Northern Region of Thailand", International Trade & Academic Research Conference (ITARC) - London 2010, DBA Marketing Program, Payal University, Thailand.*
- *Ajibola Olakunle Anani (2010), "Attracting and Retaining Customers in South Africa"s Banking Sector", Ph. D. Thesis submitted at Business School in the Faculty of Business and Economic Sciences of the Nelson Mandela Metropolitan University, South Africa.*
- *Vaidya, Shripad Ramakant (2011), "Emerging Trends on Functional Utilization of Mobile Banking in Developed Markets in Next 3-4 Years", International Review of Business Research Papers, Vol. 7, No.1, January 2011, pp. 301-312.*
- *Malarvizhi, V. and Rajeswari, A. (2012)., "User"s Criteria for selecting Mobile Banking Services in Coimbatore, Empirical Evidence, Volume 1, Issue 1, Journal of Asian Research Consortium, February, ISSN: 2249-7315*
- *Lalitha. B. S. (2014), "Customers" Adoption of latest Innovative Products and Services in Indian Retail Banks", EXCEL International Journal of Multidisciplinary Management Studies, ISSN: 2249-8834, EIJMMS, Vol. 4 (2), February.*
- *http://en.wikipedia.org/wiki/Mobile_banking (accessed on 05-01-2012)*
- *http://www.articlesbase.com.html (accessed on 06-01-2012)*
- *http://www.rbi.org.in/ (accessed on 05-01-2012)*
- *https://www.sbi.co.in/ (accessed on 24-10-12)*
- *http://www.bizresearchpapers.com/22.%20Shripad-FINAL.pdf(accessed oN 09-02-13*
- *http://en.wikibooks.org (accessed on 06-03-13)*
- *http://aut.researchgateway.ac.nz/handle/10292/666 (accessed on 06-03-13)*

Use of Mobility Modeling in Manet's & Wireless Networks

Mr. Shashiraj Teotia[1], Ms. Samridhi Sharma[2], Ms. Nitasha Verma[3]

[1] Assistatnt Professor-Department of Computer Application,S.V. Subharti University, Meerut

[2] Lecturer-Department of Computer Application, S.V. Subharti University, Meerut

[3] Assistatnt Professor-Department of Computer Application, S.V. Subharti University, Meerut

ABSTRACT

Mobility modeling management is the cornerstone of wireless networks philosophy. Mobility analysis gives a deep insight on the impact of the terminal mobility on the cellular system performance. In third generation mobile communication systems, the influence of mobility on the network performance will be strengthened, mainly due to the huge number of mobile users in conjunction with the small cell size. In particular, the accuracy of mobility modeling becomes essential for the evaluation of system design alternatives and network implementation cost issues. Currently available mobility models tend to be either too simplifying or too sophisticated. For mobility modeling under realistic traffic and environmental conditions, this thesis introduces a novel representation technique which uses the distribution functions of street length, direction changes at crossroads, and terminal velocity. Other important factors influenced by user mobility concern the mobile user calling behavior expressed by the incoming/outgoing call arrival rate and average call duration. This is capable to describe the user behavior in detail, and is applied for the characterization of the traffic in individual single cells of the mobile network. The effect of mobility has been analyzed in terms of the local performance measures like probability of handover and call blocking probability (for new and handover calls). Additionally, this model has been used to calculate the distribution of channel holding times. The performances of new call handling algorithms are evaluated. The global performance criteria of interest are call dropping probability for all calls, call processing

Keywords - MANET, Wireless Networks, Mobility Models

1. INTRODUCTION

1.1 OVERVIEW OF MOBILE AD-HOC NETWORKS (MANET):

A mobile ad hoc network (MANET), is a self-configuring infra structure less network of mobile devices connected by wireless links. In Latin ad-hoc means "for this purpose only".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic..

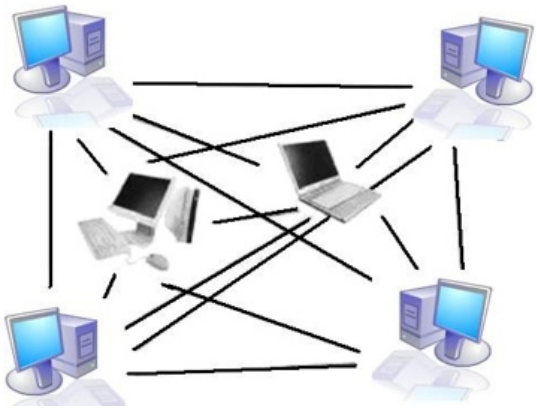

Figure 1.0 Mobile Ad-Hoc Network

1.2 OVERVIEW OF WIRELESS NETWORKS:

Wireless network have become increasingly popular in the computing industry since 1970. It is particularly true within the past decade, which has seen wireless networks being adapted to enable mobility. The area of wireless communication has been and is continuing to develop at a rapid pace over the years. The most Wireless network of today consists of cells. Each cell contains a base station, which is wired to a fixed wire network. The base stations interact with the portable handheld devices and provide these devices the wireless link to the network.

Figure 1.1: Internet at Mobile Handset

1.3 OVERVIEW OF MOBILITY MODEL:

Mobility models are represented by the movement of mobile users, and they change their location, velocity and acceleration overtime. These models are used for simulation purpose. For mobility modeling, the activity of a movement of user can be described using both analytical and simulation models.

When evaluating mobility models for wireless ad hoc networks with respect to performance or functional correctness, several assumptions have to be decided upon. Such assumptions may include the size and shape of the area used by the wireless devices, their transmission ranges and their movement pattern including allowed directional changes and speeds.

1.4 STUDY OF EXISTING MOBILITY MODEL:

Mobility models represent the movement of mobile users and how their location, acceleration and velocity change over time. Such models are frequently used for simulation purpose when new communication techniques are investigated. Mobility management schemes for mobile communication systems make use of mobility models for future user positions.

For mobility modeling, the behavior of a user's movement can be described using both analytical and simulation models. The input to analytical mobility models are simplifying assumptions regarding the movement behaviors of users. Such models can provide performance parameters for simple cases through mathematical calculations.

1.5 PURPOSE OF MOBILITY MODEL:

The purpose of mobility models is to describe typical terminal movement so that the analysis for these purposes can be made. Thus, the movement pattern of user plays an important role in performance analysis of mobile and wireless networks, especially in third-generation mobile communication (Jonahing Kim, 2005). One frequently used mobility; model in MANET simulations is the Random Waypoint Model (Broch et al., 1998), in which nodes move independently to a randomly chosen destination with a randomly selected velocity. The simplicity of Random Waypoint model may have been one reason for its widespread use in simulations. Hence, recent research has started to focus on the alternative mobility models with different mobility characterstics. In these models, the movement of a node is more or, less restricted by its history, or other nodes in the neighborhood or the environment.

1.6 MODIFICATION OF EXISTING MOBILITY MODEL:

To produce a real-world environment within which an adhoc network formed among a set of nodes, there is a need for the modification of realistic, generic and comprehensive mobility models. Simulation environment is an important tool for the evaluation of new concepts in networking. Here we show the modified mobility model has a significant impact on network performance, especially when compared to other mobility models. The mobile adhoc networks depend on understanding protocols from simulations, before these protocols are implemented in a real world setting.

1.7 CATEGORY OF MOBILITY MODELS:

There are two types of Mobility Models.

1.7.1 Traces Based Mobility Models

Traces are those mobility patterns that are observed in real-life systems. Traces provide accurate

information, especially when they involve a large number of participants and an appropriately long observation period. However, new network environments (e.g., ad hoc networks) are not easily modeled if traces have not yet been created.

1.7.2 Synthetic Mobility Models

Synthetic models attempt to realistically represent the behaviors of MNs without the use of traces. Therefore, various researchers proposed different kinds of mobility models, attempting to capture various characteristics of mobility and represent mobility in a somewhat realistic fashion. Much of the current research has focused on the so-called synthetic mobility models (Camp et al., 2002).

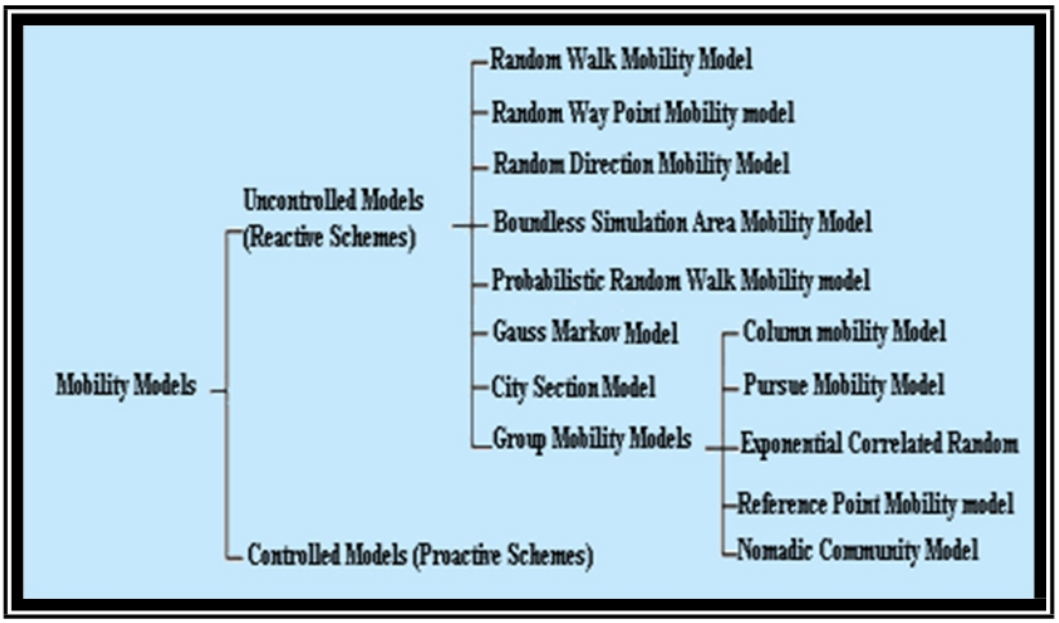

Figure 1.2: Classification of Mobility Models

2.0 LEVELS OF MOBILITY

In static networks, the mobility of nodes, users, and the monitored phenomenon itself is minimal or ignored. For example, sun and temperature sensors in a sunroom may collect relevant information and use it to control motorized shades in order to maintain these parameters within preset limits. This static paradigm may be expanded by introducing mobility in one or more of the below-mentioned three levels of the ad hoc networks:

2.1 NODE LEVEL MOBILITY

The ad hoc nodes themselves may be moving. Examples include nodes mounted on moving cars or flying unmanned aerial vehicles, collecting information as their carriers constantly change their location and/or orientation.

2.2 INFORMATION LEVEL MOBILITY

The event (source) monitored by or occurring in the network is mobile. For example, the smog ed to virtually any mobile ad hoc network at any layer (from the MAC up to the application layer).

generated by a poorly maintained truck is moving along with the truck. Another example may be the evolution of an oil spill that we try to model through measurements at distinct buoy locations.

2.3 USER LEVEL MOBILITY

Users (destination) accessing the information collected by the network may themselves be moving, and thus the information that is pertinent to them may change over time. For example, monitoring the traffic conditions on the way to the nearest hospital changes as the user is changing his/her position.

3.0 ADVANTAGES OF MOBILITY MODELS

x3.1 MOBILITY HELPS SECURITY

Security and mobility seem to be at odds with each other. Security is usually enforced by a static, central authority that is generally in charge of securing the system under consideration, be it a communication network, an operating system, or the access system to the vault of a bank. In this case, because users are static as well, their locations are predictable, they are more likely to be available, and the system can more easily perform appropriate controls. However, this intuition can be misleading: mobility, far from being a hurdle, can be useful to establish the security associations between any two mobile nodes of a given network. The idea that mobility can help security is extremely straightforward, as it simply mimics human behavior: if people want to communicate securely, they just get close to each other in order to exchange information and to establish (or reinforce) mutual credentials. In spite of its simplicity, this idea is very powerful, as it can be applied to virtually any mobile ad hoc network at any layer (from the MAC up to the application layer).

3.2 MOBILITY ENLARGES NODE COVERAGE

Many works on the coverage of mobile node networks focus on algorithms to reposition nodes in order to achieve a static configuration with an enlarged covered area. As time goes by, a position is more likely to be covered; targets that might never be detected in a stationary node network can now be detected by moving nodes. The main metrics to measure node coverage could be the area coverage at specific time instants and during time intervals, as well as the time it takes to detect a randomly located stationary target. Exploiting mobility, both metrics can be improved.

3.3 MOBILITY REDUCES UNCERTAINTY

Uncertainty increases the transaction cost and decreases the acceptance of communication and cooperation. Our objective is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship is sustained. One key way to efficiently reduce uncertainty is to exploit one important property of MANETs mobility. Node movement can increase

scope of direct interaction and recommendation propagation, hence speeding-uptrust convergence. We study this effect under different mobility models and analyze several factors that will strongly influence the convergence speed and cost. We present a detailed design of a two-level Mobility-Assisted Uncertainty Reduction Scheme (MAURS). It exploits configurable level partition and movement schemes to provide a range of trade-offs between convergence time, cost, and uncertainty level.

REFERENCES

1. *W.T. Poon, E. Chan, "Traffic Management in Wireless ATM Network Using a Hierarchical Neural-Network Based Predication Algorithm", Proc., 15th International Conference on Computers and their Applications, March 2000,*
2. *J.Chan, B. Landfeldt, A. Seneviratne, P. Sookavatana, "Integrating Mobility Prediction Preallocation into a Home-Proxy Based Wireless Internet Framework", Proc., IEEE International Conference on Networks, Sept 2000, pp. 18- 23*
3. *H. Kim, J. Jung, "A Moblity Prediction Handver Algorithm for Effective Channel Assignment in Wireless ATM", Proc., IEEE GLOBECOM, Nov 2001, Volume 6, pp. 3673-3680*
4. *A. Aljadhai, T. F. Znati, "Predictive Mobility Support for QoS Provisioning in Mobile Wireless Environments", IEEE Journal on Selected Areas in Communications, Oct 2001, Vol 19, No 10,pp. 1915-1930.*
5. *A. Bhattacharya, S. K. Das, "LeZi-Update: An Information-Theoretic Framework for Personal Mobility Tracking in PCS Networks", Wireless Networks 8, 2002, pp. 121-135*
6. *B. P. V. Kumar, P.Venkataram, "Prediction-based Location Management using Multilayer Neural Networks", J. Indian Inst. Sci., 2002, 82, pp. 7-21*
7. *J. Ye, J. Hou, S.Papavassiliou, "A Comprehensive Resource Management Framework for Next Generation Wireless Networks", IEEE Transactions on Mobile Computing, Fall 2002, Vol 1, No 4, pp. 249 – 264*
8. *A. Jayasuriya, J. Asenstorfer, "Mobility Prediction for Cellular Networks Based on the Observed Traffic Patterns", Proc., 2nd IASTED International Conference Wireless and Optical Communications, 2002, 356-235,*
9. *R. Chellappa, A. Jennings, N. Shenoy "A Comparative Study of Mobility Prediction in Cellular and Ad Hoc Wireless Networks", Proceedings of the IEEE Int'l Conference on Communications 2003 (ICC2003),Alaska, USA, May 2003.Yaneer Bar-Yam*
10. *(2003). Dynamics of Complex Systems, Chapter 2.Yaneer Bar-Yam*
11. *(2003). Dynamics of Complex Systems, Chapter 3.Yaneer Bar-Yam*
12. *(2005). Making Things Work. See chapter 3.*
13. *A. Kivi, "Mobile Data Service Usage Measurements - Results 2005- 2007", COIN National Project - Helsinki University of Technology, 2008 Project Report, http://www.netlab.hut.fi/tutkimus/coin/.*
14. *Q. Huang, S. Chan and M. Zukerman, "Improving Handoff QoS With or Without Mobility Prediction", IEEE Electronics Letters, Vol. 43, No. 9, April 2007.*
15. *A. Kivi, "Mobile Data Service Usage Measurements - Results 2005- 2007", COIN National Project - Helsinki University of Technology, 2008 Project Report, http://www.netlab.hut.fi/tutkimus/coin/.*

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.