International Journal of Electrical, Electronics and Mechanical Controls
ISSN (Online) : 2319-7501
Volume 3 Issue 2 May 2014
Manuscript ID : ISSN23197501-V3I2M5-052014

A PRAGMATIC REVIEW OF MALICIOUS NODES AND SECURITY ASPECTS IIN MOBILE AD HOC NETWORKS

Jamal kh-Madhloom al-bdairi (M.Tech.)
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India

Rohit Vaid
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India

ABSTRACT

Wireless communication is becoming more popular among the users now a days and this is mainly due to the technological revolution in the field of mobile phones, laptops, PDA, wireless LAN and modems. There are two different approaches to establish the communication among a number of hosts. First approach is to use an existing cellular hierarchy which carries data as well as voice; in the cellular network, there is a centralized administration or a fixed base station which handles routing and resource management procedures, since all the routing decisions are made in a centralized manner. Therefore these networks are also called Infrastructural based networks. But the main problem here is handoff between two areas when user moves from one cell to other. It becomes an important to transfer data without any delay while handoff. Another main problem is that it is limited to the area where network is present. In the second approach we can form an ad hoc network among all users who wants to communicate with each other. This means all the users in the ad hoc network must be willing to forward data packets to make sure that the packets are delivered from the source to destination. This form of networking is smaller than the cellular approach and only limited in the range by the individual nodes transmission range. This system has its own advantages over cellular system and these are On demand setup, Fault tolerance and Unconstrained connectivity. This manuscript highlights various security issues associated with mobile ad hoc networks.

Keywords – Mobile Ad Hoc Network, Security Measures

INTRODUCTION

A mobile ad hoc network (MANET) are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure, hence they are also called Wireless infrastructure less networks. It consists of mobile nodes that use a wireless interface to communicate with each other. As all the routing decisions are made by the nodes itself. Therefore, in an ad hoc network the mobile nodes serve as both hosts and routers so they can forward packets on behalf of each other.

Mobile Ad-hoc Network (MANET) is defined as the moving node rather than any fixed infrastructure, act as a mobile router. These mobile routers are responsible for the network mobility. The history of mobile network begin after the invention of 802.11 or WiFi they are mostly used for connecting among themselves and for connecting to the internet via any fixed infrastructure. Vehicles like car, buses and trains equipped with router acts as nested Mobile Ad-hoc Network.

Vehicles today consists many embedded devices like build in routers, electronic devices like Sensors PDAs build in GPS, providing internet connection to it gives, information and infotainment to the users. These advances in MANET helps the vehicle to communicate with each other, at the time of emergency like accident, or during climatic changes like snow fall, and at the time of road block, this information will be informed to the nearby vehicles.

Nowadays technologies rising to provide efficiency to MANET users like providing enough storage space, as we all know the cloud computing is the next generation computing paradigm many researches are conducting experiments on Mobile Ad-hoc Network to provide the cloud service securely.

CHALLENGES WITH MANET

Regardless of the attractive applications, the features of wireless networks introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include:

- **Routing:** Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.
- **Security and Reliability:** In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics also introduce reliability problems, because of limited wireless transmission range, broadcast nature of the wireless medium (e.g. hidden terminal problem), and mobility-induced packet losses and data transmission errors.
- **Quality of Service (QOS):** Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. .
- **Power Consumption:** For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration

APPLICATIONS

Due to their quick and economically less demanding deployment, find applications in several areas, some of these include are:

- **Mobile conferencing:** Ad hoc networks enable mobile conferencing for business users who need to collaborate outside their office where no network infrastructure is available. There is a growing need for mobile computing environments where different members of a project need to collaborate on design and development. The users need to share documents, upload and download files, and exchange ideas.
- **Personal area and home networking**: Ad hoc networks are quite suitable for home as well as personal area networking applications. Mobile devices with Bluetooth or WLAN cards can be easily configured to form an ad hoc network. With the Internet connectivity at home, these devices can easily be connected to the Internet. Hence, the use of these kinds of ad hoc networks has practical applications and usability.
- **Emergency services:** When the existing network infrastructure has ceased to operate or is damaged due to some kind of disaster like earthquakes, hurricanes, fire, and so forth, ad hoc networks can be easily deployed to provide solutions to emergency services. These networks can also be used for search and rescue operations, retrieval of patient data remotely from hospitals and many other useful services.
- **Public hotspots:** In places like airports In places like airports, train stations, coffee shops, and pubs, football grounds, and malls, ad hoc networks provide users the ability to create their own network and communicate with each other instantly. Ad hoc networks can also be used for entertainment purposes like providing instant connectivity for multi-user games
- **Military applications:** In battlefield, sensor network can be deployed for communications among the soldiers in the field. Different military units are expected to communicate and cooperate with each other within a specified area. In these kinds of low mobility environments, sensor network is used for communications where virtually no network infrastructure is available.
- **Mobile commerce:** Ad hoc networks can be used to make electronic

payments anytime, anywhere. Business users can retrieve customer/sales-related information dynamically and can build reports on the fly.

INTRUSION DETECTION

Data Mining based methods Anomaly based IDS have the ability to detect new attacks, as any attack will differ from the normal activities. In order to detect attacks, a number of clustering based detection methods has been proposed.

a. **PEA Algorithm:** A parallel clustering ensemble algorithm for IDS achieve the high speed, high detection rate and low false alarm rate. The parallel clustering ensemble is based on evidence accumulation algorithm. The evidence accumulation combines the results of multiple clustering into a single data partition, and then detects intrusions with it.
b. **Hybrid Anomaly Detection System**: This system was proposed which combine k-means, and two classifiers: k-nearest neighbor and naive bayes. Firstly, it performs the feature selection process from intrusion detection data set using an entropy based feature selection algorithm which selects the important attributes and removes the redundant attributes. The next step is cluster formation using k-Means and then it further classifies them by using a hybrid classifier.
c. **Boosted Decision Tree Approach:** A new ensemble boosted decision tree approach has proposed for IDS which is a learning technique that allows combining several decision trees to form a classifier which is obtained from a weighted majority vote of the classifications given by individual trees. D. SVM Support vector machines (SVM), is a classification method that perform very well in terms of text classification. The basic SVM [44] deals with two-class problems in which the data are separated by a number of support vectors. Support vectors are the subset of training data that is used to define the boundary between the two classes.
d. **Watchdog:** Martiet al. proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the

Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

e. **TWOACK:** With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR)

f. **AACK:** Based on TWOACK, Sheltamiet al. proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

g. **MANETs face security risks and energy consumption:** So monitoring security measurement is big issues in front of MANET. And This challenge has been become bigger due to limited battery backup. To address this issue, paper [50] develops two methods for aggregation, named lossless and lossy aggregation techniques. This will reduce the requirement of the energy too, while preserving the desired detection accuracy.

MANET SECURITY ATTACKS

Malicious node is one which causes attacks on various layers on MANET like application layer, data link layer, physical and network layer.

There were two types of attacks on MANET, they are

- Active attacks
- Passive attacks

Active attacks: In this attack, some harmful information is injected into the network, which causes malfunctioning of the other nodes or network operation. For performing this harmful information it consumes some sort of energy from other nodes, those nodes are called as malicious node.

Passive attacks: In this passive attack, the malicious nodes disobey to perform its task for some sort reasons like saving energy for its own use of moving randomly, by diminishing the performance of the network.

a. **Network layer attack:** Let us concentrate on various attacks on the network layer.

Wormhole attack: Wormhole attack is also known as tunneling attack, in this tunneling attack the colluding attackers build tunnel between the two nodes for forwarding packets claiming that providing shortest path between the nodes and taking the full control of the nodes, which is invisible at the higher layers.

Black hole attack: Black hole attack is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path. In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

- **Resource consumption attack:** In the resource consumption attack, a malicious node can try to consume more battery life demanding too much of route discovery, or by passing unwanted packets to the source node.
- **Location disclosure attack:** In the location disclosure based attack, the malicious node collects the information of routes map and then focus on further attacks. This is one of the unsolved security attacks against MANETs.

b. Multi layer attacks in MANET: There are different types of multilayer attacks in MANET, they are as follows

- Denial of Service (DoS)
- Jamming
- SYN flooding
- Man In Middle attacks
- Impersonation attacks

- **Denial of service (DoS) attacks:** In this type of attacks, the attacker injects enormous amount of junk packets into the network which leads to the loss of network resources and causes congestion among the wireless networks.
- **Jamming:** Jamming is known as the DoS attack that affect communication between two nodes, the main goal of jamming is to block the valid user's like sender and receiver from transmitting and receiving packets, jamming is divided into two types
  - Physical jamming attacks
  - Virtual jamming attacks

Physical jamming: Physical jamming is caused by continuous transmission of packets to the receiver or by causing packet collision at the receiver. Physical jamming is also known as radio jamming, radio jamming is simple attack causing more disrupt to the authorized users. Jammers causing this attack block the authorized users from accessing the wireless channel by controlling the wireless medium. The nodes trying to communicate strangely waiting for the carrier sense timing of the channel to become idle. This put the nodes into list of larger exponential back off period.

Virtual Jamming: Virtual jamming is most often possible at the MAC (Medium Access Control) layer, causing affects on Rate to send (RTS) frames, or Clear to send (CTS) frames, or data frames. One of the advantage of this attack is it consumes less power than comparing to physical or radio jamming. In virtual jamming the malicious node try send RTS command continuously on the transmission with more number of times. In this process the malicious node blocks the transmission limited amount of power. This attack more dangerous than that of physical attack, by sending false frames it will disturb other node from accessing for certain period of time.

SYN flooding attack: Synchronization (SYN) flooding attack, In this attack a malicious node sends enormous amount of synchronization packets to the affected node and by faking the address of synchronization packets. An SYN-ACK message was sent out from affected node after it receives SYN packets from the attacker, without getting any response from malicious node, the half open request remains in the affected node. The victim node stores this connection in fixed size table while it waits for the acknowledgement, with all these pending connection, the affected node not be able to accept any other valid attempts to open a connection. Normally the half open connection automatically expires at certain period of time, but the malicious node continuously sends the packets before the previous connection expires. Some of the counter measures to prevent SYN flooding attacks are:

- Filtering
- Firewalls and proxies

Filtering: The filtering techniques are described in the RFC 2827. The most effective technique to prevent SYN flooding is the ingress filtering. It prevents the spoofed IP address. But this technique is not reliable because it is not universally accepted.

Firewalls and proxies: These firewalls and proxies prevent the SYN flooding attack from network attacker using two techniques

- ✓ Spoofing initiators SYN-ACK
- ✓ Spoofing ACK to the listeners

Man in the Middle attacks: Man in the Middle (MITM) attack is commonly known as bucket brigade attack, in this attack the malicious node makes independent connection for relaying message between the victims node, makes them believe that they are messaging through a private network. This attack is also commonly known as fire brigade attacks. In this a bucket of water is passed from one person to another person to put out the fire. Secure socket layer (SSL) helps in preventing MITM attacks; it is based on public key cryptography. It includes:

- SSL architecture
- SSL alert protocol
- SSL hand shake protocol
- SSL Architecture

SSL Handshake protocol

- ✓ It helps intervention of security algorithms and parameters.
- ✓ It performs the key exchange.
- ✓ It helps in performing server authentication and sometimes client authentication.

SSL Record protocol

- ✓ It helps in fragmentation of address.
- ✓ It helps in compression of protocol address.
- ✓ It performs integrity protection and authentication of message.
- ✓ It helps in the encryption of message.

SSL Alert protocol: It will perform the fatal alert warning. The message consist of two fields

Warning: It includes commands like no certificate, close notify, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown

Fatal: It includes commands like decompression failure, hand shake failure, illegal parameter, unexpected message, bad record MAC

LITERATURE REVIEW

To propose and defend the research work, a number of research papers are analyzed. Following are the excerpts from the different research work performed by number of academicians and researchers.

IEEE TRANSACTIONS ON MOBILE COMPUTING - On the Security of Route Discovery in MANETs Mike Burmester, Member, IEEE, Breno de Medeiros Member, IEEE - Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes, that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from an efficiency and from a security point of view. Recently, a security model tailored to the specific requirements of MANETs was introduced by Acs, Butty ´an, and Vajda. Among the novel characteristics of this security model is that it promises security guarantees under concurrent executions, a feature of crucial practical implication for this type of distributed computation. A novel route discovery algorithm called endair. A was also proposed, together with a claimed security proof within the same model.

IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 241 Manuscript received August 5, 2009 Manuscript revised August 20, 2009 MANET Security Issues Nishu Garg et. Al. - When a routing protocol for manet Networks (mobile and ad hoc networks) does a route discovery, it does not discover the shortest route but the route through which the route request flood traveled faster. In addition, since nodes are moving, a route that was the shortest one at discovery time might stop being so in quite a short period of time. This causes, not only a much bigger end-to-end delay, but also more collisions and faster power consumption. In order to avoid all the performance loss due to these problems, this paper develops a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol. It also shows how the same mechanism can be used as a bidirectional route recovery mechanism. We consider the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPSec are not applicable. We look at AODV in detail and develop a security mechanism to protect its routing information. We also briefly discuss whether our techniques would also be applicable to other similar routing protocols and about how a key management scheme could be used in conjunction with the solution that provide.

International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012 65 Network Security for MANETS, Mamatha. T - A mobile ad hoc network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without the help from a network infrastructure. Although security issues in mobile ad hoc networks have been a major focus in the recent years, the development of fully secure schemes for these networks has not been entirely achieved till now. MANETs have a unique characteristics and constraints that make traditional approaches to security inadequate. The lack of an infrastructure exacerbates the situation of using shared secret keys or authentication among members. Therefore, the issues of authentication, key distribution and intrusion detection require different methods, which are discussed here. In this paper, we propose to combine efficient techniques from elliptic curve cryptography (ECC) and a distributed intrusion detection system (IDS) based on threshold cryptography. And also propose to use a distributed certifying authority (CA) along with per-packet per-hop authentication for addressing the issues mentioned above. The model assumes that no single node can be trusted and relies instead on a distributed trust model. Keywords- mobile ad hoc network (MANET), elliptic curve cryptography (ECC), distributed certifying authority, certifying authority (CA), threshold cryptography, intrusion detection (ID)

Routing Security in Mobile Ad-hoc Networks Issues in Informing Science and Information Technology Volume 9, 2012, Jonny et. Al. The role of infrastructure-less mobile ad hoc networks (MANETs) in ubiquitous networks is out-lined. In a MANET there are no dedicated routers and all network nodes must contribute to routing. Classification of routing protocols for MANET is based on how routing information is acquired and maintained by mobile nodes and/or on roles of network nodes in a routing. According to the first classification base, MANET routing protocols are proactive, reactive, or hybrid combinations of proactive and reactive protocols. According to the role-based classification, MANET routing protocols are either uniform when all network nodes have the same role or non-uniform when the roles are different and dedicated. A contemporary review of MANET routing protocols is briefly presented. Security attacks against MANET routing can be passive and or active. The purpose of the former is information retrieval, for example network traffic monitoring, while the latter is performed by malicious nodes with the express intention of disturbing, modifying or interrupting MANET routing. An overview of active attacks based on modification, impersonation/spoofing, fabrication, wormhole, and selfish behavior is presented. The importance of cryptography and trust in secure MANET routing is also outlined, with relevant security extensions of existing routing protocols for MANETs described and assessed. A comparison of existing se-cure routing protocols form the main contribution in this paper, while some future re-search challenges in secure MANET routing are discussed.

CONCLUSION

A MANET is a special type of ad hoc network that can change position, direction, locations and configure itself on the fly i.e. dynamically. As MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. An assorted stack of protocols and techniques are used for accomplishing the task of security and privacy in MANETs. But the proposed work is implemented with a unique set of tasks and steps. There are number parameters or metrics which are required be considered for the integration and analysis of security aspects.

REFERENCES

[1] T.H Clausen, “Introduction to Mobile Ad-hoc Networks (MANET)s” , 2007.

[2] “Wi-Fi (wireless networking technology)” published in encyclopaedia, 2002.

[3] Che-Fn Yu, “Security safe guards for intelligent networks”, GTE laboratories incorporated, 40 sylvan road, Waltham, MA 02254.

[4] V. Venkata Ramana, Dr. A. Rama Mohan Reddy, and Dr. K. Chandra Sekaran, “Bio Inspired Approach to Secure Routing in MANETs”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, July 2012

[5] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, “WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”, International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2008.

[6] Tuna Guven, Hui Zeng, Jason H. Li, Song Luo, Subir Das, Tony McAuley, Thomas Stuhrmann, Joe Sherrick, Christine Adelfio, Seth Spoenlein, Aristides Staikos, Mario Gerla, "A Multi-Layer Approach For Seamless Handoff In Ad Hoc Networks With Wireless Heterogenity", IEEE, Paper ID 900668.pdf.

[7] D.Suresh kumar, K.Manikandan, M.A.Saleem Durai, "Secure On-Demand Routing Protocol for MANET using Genetic Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 19– No.8, April 2011.

[8] S. Prasad, Y.P.Singh, and C.S.Rai, " Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[9] Poonam Garg, "A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009

[10] Lu Han, Dongming Zhaow, and Manli Zhou, "A Network Layer Security Mechanism Based on Collaborative Intelligent Agents in MANET" IEEE,2005

[11] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism", International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", international conference on wireless networks, 2003

[13] Marek Hejmo, Brian L. Mark, Member, IEEE, Charikleia Zouridaki, Student Member, IEEE, and Roshan K. Thomas, "Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs", IEEE Transactions On Vehicular Technology, Vol. 55, No. 3, May 2006

[14] Arif Sari and Dr. Beran Necat, “Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012

[15] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav. ” Flooding Attacks Prevention in MANET”, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3

[16] Dimitris Mitropoulos and Diomidis Spinellis, “Securing e-voting against MITM attacks”, 13th Panhellenic Conference on Informatics, Corfu, Greece, September 2009

[17] Latha Tamilselvan and Dr. V. Sankaranarayanan, “Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[18] Manel Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector Routing”, Mobile Computing and Communications Review, Volume 6, Number 3.

[19] Dr. C. Anbalagan and Mr. T. Sugantha, “Implementation of Evolutionary Algorithms in Different Methods of Research- A Analytical Approach with Selection, Recombination, Mutation,

[20] Reinsertion and Population Model, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.1, No. 1, October 2011.