A Survey on Performance And Security In Mobile Ad Hoc Networks

Navneet Kumar[1], Prof. S R Yadav[2]

[1]PG Scholar, [2]Head Hod PG, CSE

MITS, Bhopal (India)

Abstract - Mobile Ad hoc Network (MANET) is a new field of communication operating in an extremely unpredictable and dynamic environment. These networks are gaining increasing popularity in recent years because of their ease of deployment. A MANET consists of collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration. In ad hoc networks, routing protocols are challenged with establishing and maintaining multi-hop routes with security in the face of mobility, bandwidth limitation and power constraints. The work is concentrated primarily on the provision of security in the On-demand routing protocols like Dynamic Source Routing (DSR) ,Ad hoc On Demand Vector (AODV) and since they are efficient for routing in large ad hoc networks and they initiate and maintain the routes that are currently needed. The work proposes the application of Dual Hash Authentication Technique (DHT) in association with Self-Healing and Optimizing Routing Technique (SHORT) in AODV. In Dual Hash Authentication, one hash function is used to authenticate the received routing packets and the other one is used to prevent the current nodes modifying the routing information themselves. SHORT helps all the neighbouring nodes to monitor the route and try to optimize itself, if a better local sub-path is available. The work also proposes Triple Hash Authentication Technique (THT) which is almost similar to DHT but included HMAC authentication for the third one between the destination node and source node. This THT is also applied to the on-demand routing protocols as mentioned above. In addition to the above techniques, Digital Signature mechanism is applied to the routing protocol DSR and its performance is compared with DSR and AODV. The work further proposes the application of intrusion detection system (IDS) and GeOmetric DOMinated set algorithm(GODOM). The IDS is used to check every packet using some threshold value in order to identify the malicious packets. GODOM algorithm is used to find out the number of active nodes in which the IDS can be installed. This work is also applied to both AODV and DSR.

Keyword: - MANET, DSR, MDSR, Routing, AODV, DSDV.

1. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc. have reduced drastically. The latest trend in wireless networks is towards *pervasive and ubiquitous computing* - catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such as universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints

Of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in *mobile ad hoc networks*, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure. The rest of this chapter is organized as follows – initially a classification of wireless networks in use today is described followed by the background and origins of ad hoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. The final section gives an outline of the chapters to follow.

2. SYSTEM MODEL

2.1 Taxonomy of Wireless Networks

A wireless network in general consists of a set of mobile hosts which communicate to other mobile hosts either directly or via an access point (base station). The following is a broad classification of wireless networks-

2.1.1 Wireless LANs and PANs

A Wireless Local Area Network (WLAN) consists of a set of mobile users communicating via a fixed base station or an access point. The mobile node can be any device such as a palmtop, PDA, laptop etc. as shown in Figure 1.1.

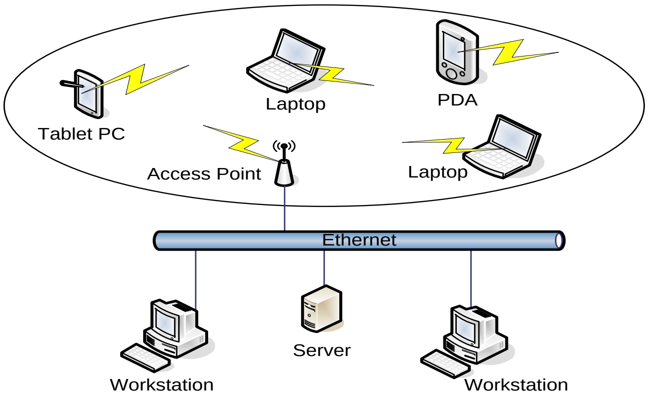

Figure 2.1.1: Wireless LAN

Such networks are usually deployed in offices, cafeterias, universities, etc. and are most prevalently used nowadays. There are three types of WLANs – Independent Basic Service Set (**IBSS**), Basic Service Set (**BSS**) and Extended Service Set (**ESS**). A detailed classification is beyond the scope of this thesis. IEEE 802.11 is an adopted international standard for wireless LANs which provides transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The latest version of this standard in use today is IEEE 802.11g which provides a bandwidth of up to 54 Mbps.

A Wireless Personal Area Network (WPAN) consists of personal devices which communicate without any established infrastructure. The IEEE 802.15.1 standard for Wireless Personal Area Networks, also called popularly as the Bluetooth is currently being used for short range communication such as in digital cameras, PDAs, laptops, etc.

2.1.2 Wireless WANs and MANs

Nowadays, the trend is towards a *wireless internet* consisting of mobile nodes accessing the internet without the help of any backbone network. This type of network is based on the *cellular* architecture in which a large area to be covered is divided in to several cells, each having a fixed base station. Each cell consists of several mobile terminals (MT) which communicate to other mobile terminals in a same cell through the base station as shown in Figure1.2.

The communication between nodes in different cells is carried on by a procedure called *handoff* which involves communication between the base stations in the two cells. Cellular networks have constantly evolved from the First Generation Cellular Systems (1G) to the Third Generation Systems (3G). Today, most wireless data communication takes place across 2G cellular systems such as TDMA, CDMA, PDC, and GSM, or through packet-data technology over old analog systems such as CDPD overlay on AMPS [1]. Although traditional analog networks, having been designed for voice rather than data transfer, have some inherent problems, some 2G (second generation) and new 3G (third generation) digital cellular networks are fully integrated for data/voice transmission. With the advent of 3G networks, transfer speeds should also increase greatly.

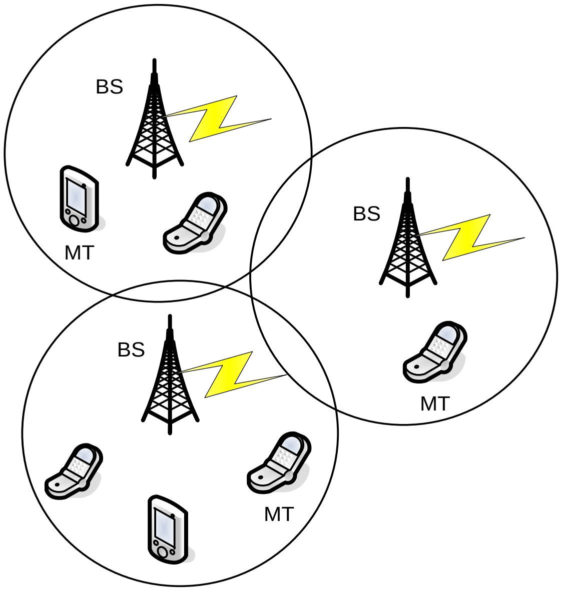

Figure 2.1.2: A Cellular network

Wireless Metropolitan Area Networks (WMANs) are networks that typically span several kilometers and cover large parts of cities. The IEEE 802.16 which is based on the OSI model is a standard used for such types of networks. It is mostly used for real time data and multimedia applications such as digital video and telephony.

Wireless WANs, which can bridge branch offices of a company, cover a much more extensive area than wireless LANs. In wireless WANs, communication occurs predominantly through the use of radio signals over analog, digital cellular, or PCS networks, although signal transmission through microwaves and other electromagnetic waves is also possible.

2.1.3 Mobile Ad hoc and Sensor Networks

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure.

As shown in Figure.1.3, there are no base stations and every node must co-operate in forwarding packets in the network.

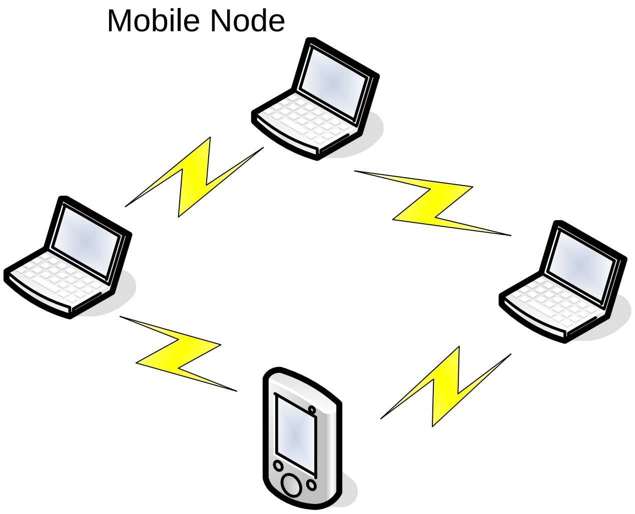

Figure 2.1.3: A Mobile ad hoc Network

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes.

2.2. Ad Hoc Routing Protocols

A. Ad hoc On Demand Distance Vector (AODV)

As the name of AODV indicates, it operates only when it is requested. The packets are transferred through the active route within the past active timeout period. AODV broadcasts a route request (RREQ) in the network, when there does not exist an active route between source and destination. The RREQ is received by all the nodes in the network. All the nodes receiving the RREQ, send a route reply (RREP) to the source so as to generate the route for packet transmission [4].

When all the RREPs are received by the source, the source has to select the best route for the transmission. A route is active only for the transmission period, when the transmission is completed or the source stops sending the packets the route discards. Due to the mobile nodes, the routes between the nodes break with the movement of the nodes, so the topology changes in the network. AODV alternates the routes in respond to the route breakages and does not stop the transmission.

A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care.

B. Dynamic Source Routing (DSR)

Dynamic Source Routing is specially designed for the networks having mobile nodes. In DSR, two mechanisms work together for the packet transmission, i.e., Route Discovery and Route Maintenance. Route Discovery is used when a source wants to send a packet to the destination but does not have a route, Route Discovery finds a route for the packet transmission. Due to the mobile nodes in MANET, the positions of the nodes changes frequently that results in route breakage, in that case, Route Maintenance is used, it detects other routes that leads the packet to the destination [6]. DSR works well even with high mobility rates and also responds well in large networks of 100 nodes [7].

C. Temporally Ordered Routing Algorithm (TORA)

The temporally ordered routing algorithm is a reactive routing protocol, it inhibits the following attributes [8]:

- Multipath routing,
- Loop-free routes,
- Distributed execution,
- Localization of algorithmic reaction to topological changes,
- Route establishment and maintenance.

In TORA, it is necessary for each node to maintain the adjacent routers information so that whenever a packet is to be transferred, source just search in the adjacent routers information table for a route which leads the packet to the destination. In the manner a route is established from source to the destination to transfer a packet in TORA. TORA supports both reactive and proactive routing [2].

3. RELATED WORD

Security Goals In Mobile And Hoc Networks:

Before we survey the Mobile Ad hoc network security solutions, first it is necessary to understand the goals on the basic to which we are able to understand that Mobile Ad hoc network is secure or not. First we have to survey that on what basis we want to secure Mobile Ad hoc network. There are several goals and criteria on the basic of which we can judge Mobile Ad hoc networks. Some of these are:

1. Availability

The first criterion is the availability of nodes. Each node should preserve its availability to provide all the services regardless its state of security. This security criterion is mainly challenged at the DoS attacks; this some selfish nodes make network services unavailable.

2. Integrity

When the messages are transferred integrity ensures the identity of the message, so integrity is very important criterion. Integrity depends on [9]:

I. Malicious altering
II. Accidental altering

Malicious altering means that the message can be removed, revised or replayed by attackers with malicious goals. Accidental altering means that the message is lost or its content is changed due to some failures such as transmission error in communication, hardware error or hard disk failure.

3. Confidentiality

Confidentiality is also an important criterion because it prevents the network from the unauthorized access [8]. The secret and confidential information are only accessible to authorized members.

4. Authenticity

Authenticity is mandatory to prove the identity of network users. It assures that users those are participating in communication are genuine and are not imitator.

5. Non-repudiation

Non-repudiation ensures that the receiver or sender cannot deny that have sent or receive fake message. This is helpful if we need to check the work of nodes, if a node found sending improper message means that the node is compromised.

6. Authorization

Authorization is a process of checking whether the user has authorized to access the network or not. It specifies the privileges and permissions and gives authority certificate to authorized user. Authorization is generally used to assign access rights to users at different levels

This section presents a conversation on the performance of the previously described ad hoc routing protocols. The interpretation are based on various studies that have been done to compare the performance of routing protocols for MANETs

(a) Performance of DSR

When low mobility DSR performs very well and delivers close to 95% of its packets. At high mobility, the throughput drops to about 70%. The throughput in DSR also decreases as a function of the number of nodes in the network. At high load, high mobility and large number of nodes, the throughput can be as low as 50%. The per-packet overhead in DSR is high because it embeds the complete source route in the packet header. This overhead can reach 100% for small sized data packets. DSR tend to keep the routing overhead relatively low even under high loads and large number of nodes. DSR finds close to optimal routes in most cases. Underneath low network loads, the average end-to-end delay in DSR is very low. However, the average delay can increase 5-6 times for modest to high network loads.

(b) Performance of AODV

The AODV shows well performance in networks of up to 100 nodes regardless of node mobility and network load. Under these conditions, it delivers close to 95% of its packets and the throughput can approach 100% in fairly static networks. The throughput decreases as the number of nodes increases due to longer routes and higher collision rate. At number of nodes becoming more, the throughput becoming low .The packet delivery ratio also drops with increase in nodal mobility. The routing overhead is lower than proactive protocols but is high compared to DSR. However, AODV outperforms DSR in terms of per-packet overhead. Under conditions of high mobility, high load and larger number of nodes, the throughput can drop to 70%. Unlike many protocols, AODV does not find the optimal route in most cases and the difference in the optimal route and the route found by AODV can be up to four hops. It is interesting to note that the average delay in AODV decreases as the mobility increases.

(b) Performance of TORA

When the numbers of nodes are low, TORA performs very well even at the highest rate of node mobility and delivers about 93% of its packets. TORA is based on the theory of link reversal and this can build the configuration of short lived routing loops. This problem is responsible for greater part of the packet drops in TORA. The performance of TORA suffers a ruthless joggle as the number of nodes increases and the packet delivery ratio can fall to about 9% in huge networks. TORA fails to converge in huge networks with high mobility rates and can undergo a congestive collapse. However, the performance of TORA is poor compared to protocols like DSR and AODV and it has been found that TORA had the most overhead compared to these protocols. The routing overhead in TORA is the sum of constant mobility-independent overhead (due to neighbour sensing) and variable mobility-dependent overhead.

4. PROPOSED WORK

Security solutions in the mobile Ad hoc networks:

The security issues are key concerned of Mobile Ad-hoc network can be solved by using symmetric key algorithms. The symmetric key can be shared between the sender and the receiver. It can be provided by the Key Distribution Center (KDC). This symmetric shared key can be used as an encryption as well as decryption. To understand this, let us look at figure 2.1 .When User A wants to send a message to User B, User A must encrypt the message by using the same symmetric key for User B. Later on User B will decrypt the message by using the same key.

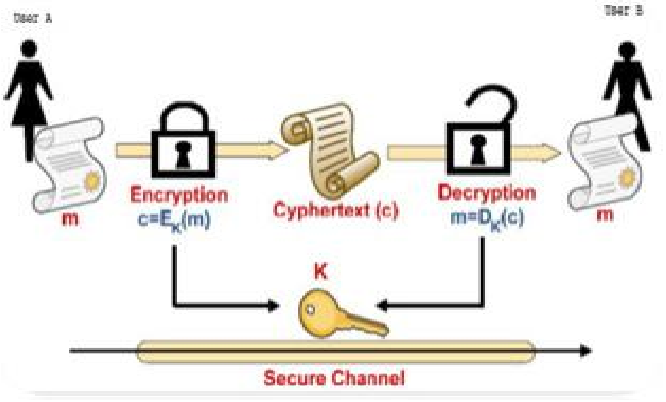

Figure 2.1: Secure Channel

By the symmetric key as a skill makes it better to be executed electronically. As the other, the symmetric algorithms can be found as non-extensive when the symmetric key is used between more than two nodes .This multiple use of key make the security of node weaker and easy to breakdown. And as solution, it is required to use another technique which is the public key cartography. Public key cryptography: there are two important keys in public key cryptography, pubic key and private key. The pubic key is usually provided among group of users while the private key is kept safe and secretly. This implies that no one apart from the authentic users knows about this key. Figure 2.2 .

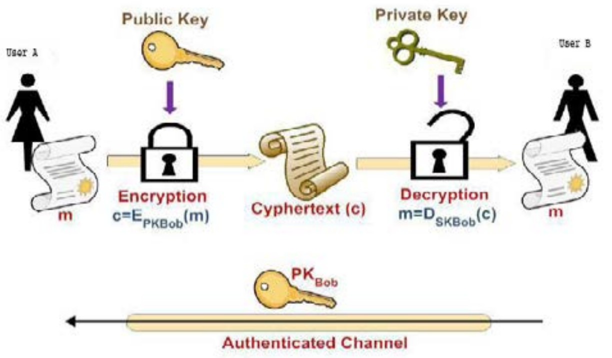

Figure 2.2: Authenticated Channel

5. RESULTS DISCUSSION

The results presented are valid for the specific scenario used in this project. Therefore, one cannot tell which of the gateway discovery methods the best one for every possible scenario is. There are many factors that can be changed and their impact should be investigated. Unfortunately the scope of this project made it impossible to deal with more than a part of these interesting issues. The aim in future work will be to examine them in greater detail. For example, changing the number of mobile nodes and the size of the topology changes the mobile node density. Its impact should be investigated. Another issue that should be examined is the impact of the number of gateways and the distance between them. Certain other questions of interest are the number of traffic sources, the number of packets sent per second, the size of the data packets, and the speed of the mobile nodes.

6. CONCLUSION

This thesis focuses on the two most important issues in mobile ad hoc networks – performance and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. The second chapter discusses some of the other challenges faced by the designers of routing protocols for MANETs. A complete understanding of these issues will help in designing efficient and effective routing protocols. It also classifies the protocols and describes a few of them.

The third chapter focuses on the second most important issue in MANETs- security. Some of the open challenges in designing a security solution are discussed, elucidating the practical implications with respect to confidentiality, integrity, availability and authenticity. The chapter then focuses on the network layer security and discusses secure routing in MANETs. It also classifies the attacks that are possible against the ordinary routing protocols and gives a threat assessment of the attacks. The second half of the chapter discusses another important aspect of security in MANETs – the key management issue. In particular, the chapter focuses on certificate-based authentication mechanisms. The requirements for an effective certificate-based authentication mechanism are identified, a survey of existing mechanisms is done and they are compared with respect to those requirements. Further, some quantitative and qualitative metrics are proposed to evaluate the mechanisms.

7. FUTURE WORK

Future work has several challenges as MANET is still evolving and securing ad-hoc network does not have any well-defined comprehensive solution in place. The main concern is that the mobile devices are battery powered and has limited storage and computational resources (Datta & Marchang, 2012). All the proposed methods/algorithm and techniques mentioned in this paper has power and processing overhead on the nodes. Hence, research in the field of hardware and resource efficiency of the node as well as algorithms which consume lesser resources are required to make the MANET security robust in nature (Datta & Marchang, 2012). On securing proto-cols researchers must work on a holistic approach to find solutions for comprehensive vulnerabilities covering from signal interception and jamming to sophisticated attacks conducted by authenticated nodes (von Mulert, et al., 2012). Moreover, such approach to include all models of known attacks and vulnerabilities would help researchers to design a more comprehensive solution rather than attack specific solutions (Datta & Marchang, 2012). Research to utilize AODV's feature to find multiple and shortest routes should be utilized to design solutions or algorithm to support the redundancy of routing where one route is infested with attacks like DoS or Link Fail-ure (von Mulert, et al., 2012).

There are no single ways through which MANET can be made secured hence, research on encrypted protocol, intrusion de-tection and access control violation should be combined to produce a future of a more secured MANET which handle large quantum of active and passive attacks.

REFERENCE

[1]. Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2]. M. Weiser, The Computer for the Twenty-First Century, Scientific American, September1991.

[3]. [3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4]. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[5]. Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[6]. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[7]. Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.

[8]. Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.

[9]. Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[10]. P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems