International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 11, (July 2013) PP: 48-53

Security issues in Mobile Ad-Hoc Networks

M. Ravi Kumar[1], Dr. N. Geethanjali[#], N. Ramesh Babu[2]
[1,2]*Research Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur*
[#]*Associate Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur*

ABSTRACT :- *MANET Is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks To accommodate the changing topology special routing algorithms are needed. There is no single protocol that fits all networks perfectly. The protocols have to be chosen according to network characteristics, such as density, size and the mobility of the nodes. There is still ongoing research on mobile ad hoc networks and the research may lead to even better protocols and will probably face new challenges. Current goal of this paper is to find out the security Issues and their Countermeasures that are adopted on the Network Layer. Network security extends computer security, thus all the things in computer security are still valid. The TCP/IP suite is the basis for today's Internet, yet it lacks even the most basic mechanisms of authentication. As usage of the Internet increases, its scarcity of built-in security becomes more and more of a problem. This paper describes serious attacks against Internet control and management protocols, with an emphasis on the ICMP protocol, as well as some of the well-known vulnerabilities of the inter-domain routing protocols.*

KEYWORDS : *MANETs, Security, Attacks, Wireless Network.*

I. INTRODUCTION

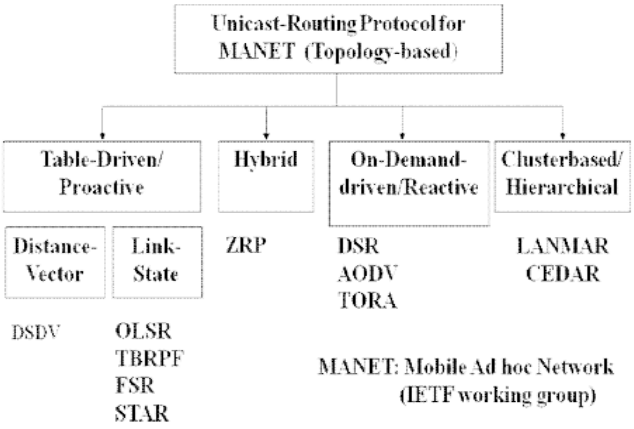
Mobile ad hoc networking is one of the more innovative and challenging areas of wireless networking, one which promises to become increasingly present in our lives. Consisting of devices that are autonomously self-organizing in networks, ad hoc networks offer a large degree of freedom at a lower cost than other networking solutions. A MANET is an autonomous collection of mobile users that communicate over relatively "slow" wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. An ad hoc wireless network should be able to handle the possibility of having mobile nodes, which will most likely increase the rate at which the network topology changes. Accordingly the network has to be able to adapt quickly to changes in the network topology. This implies the use of efficient handover protocols and auto configuration of arriving nodes.

1.1 Routing Protocols in MANETs

In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption. An Ad-hoc routing protocol is a convention or standard that controls how nodes come to agree which way to route packets between computing devices in a MANET. In ad-hoc networks, nodes do not have a priori knowledge of topology of network around them, they have to discover it. The basic idea is that a new node announces its presence and listens to broadcast announcements from its neighbors. The node learns about new near nodes and ways to reach them, and announces that it can also reach those nodes.
Routing protocols may generally be categorized as:

a. Table-driven OR Proactive routing protocols.
b. On-demand OR Reactive routing protocols.

1.2 Classification of Routing Protocols in MANETs



II. NETWORK SECURITY IN MANETS

Different variables have different impact on security issues and design. Especially environment, origin, range, quality of service and security criticality is variables that affect the security in the network. The ways to implement security vary if the range of the network varies. If the nodes are very far from each others, the risk of security attacks increases. On the other hand, if the nodes are so close to each others that they actually can have a physical contact, some secret information (e.g. secret keys) can be transmitted between the nodes without sending them on air. That would increase the level of security, because the physical communication lines are more secure than wireless communication lines. The last variable of Ad Hoc networks described with respect to security is security criticality. This means that before we think of the ways to implement security, we must consider carefully whether security is required at all or whether it matters or not if someone outside can see what packets are sent and what they contain. Is the network threatened if false packets are inserted and old packets are retransmitted? Security issues are not always critical, but it might cost a lot to ensure it. Sometimes there is trade-off between security and costs.

2.1. Problems with ad-hoc routing protocols

In ad-hoc routing protocols, nodes exchange information with each other about the network topology, because the nodes are also routers. This fact is also an important weakness because a compromised node could give bad information to redirect traffic or simply stop it. Moreover, we can say that routing protocols are very brittle in term of security. This part aims to provide a description of the causes of the problems with adhoc routing protocols.

2.1.1. Infrastructure of ad-hoc networks: Ad-hoc networks have no predetermined fixed infrastructure, that's why the nodes themselves have to deal with the routing of packets. Each node relies on the other neighboring nodes to route packets for them.

2.1.2. Dynamic topology of ad-hoc networks: The organization of the nodes may change because of the mobility-aspect of ad-hoc networks: they contain nodes that may frequently change their locations. Because of this fact, we talk about the dynamic topology of these networks, which is a main characteristic that causes problems: when several adhoc networks mix together, there can be duplications of IP addresses, and resolving it is not so simple. Then, attacks can easily occur by using this duplication of IP address (cf. attacks using impersonation)

2.1.3. Problems associated with wireless communication: Wireless channels have a poor protection to noise and signal interferences, therefore routing related control messages can be tampered. A malicious intruder can just spy on the line, jam, interrupt or distort the information circulating within this network.

2.1.4. Implicit trust relationship between neighbors: Actual ad-hoc routing protocols suppose that all participants are honest. Then, this directly allows malicious nodes to operate and try to paralyze the whole network, just by providing wrong information.

2.2 Types of Attacks in MANET

Due to their particular architecture, ad-hoc networks are more easily attacked than wired network. We can distinguish two kinds of attack: the passive attacks and the active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Instead, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The routing protocols in MANET are quite insecure because attackers can easily obtain information about network topology.

2.1.5. Attacks Using Modification: One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes. This kind of attack is based on the modification of the metric value for a route or by altering control message fields.

2.1.6. Attacks using impersonation: These attacks are called spoofing since the malicious node hides its real IP address or MAC addresses and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and then use them to announce new route (with smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants.

III. SECURITY THREATS IN NETWORK LAYER

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

3.1. Network Layer Attacks

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. Attacks at different stages are as:

1. Attacks at the routing discovery phase
2. Attacks at the routing maintenance phase.
3. Attacks at data forwarding phase.
4. Attacks on particular routing protocols.

Attacks by Names are as:

1. Wormhole attack.
2. Black hole attack.
3. Byzantine attack.
4. Rushing attack.
5. Resource consumption attack.
6. Location disclosure attack.

IV. COUNTERMEASURES

Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Hence, a variety of security mechanisms have been developed to counter malicious attacks. There are two mechanisms which are widely used to protect the MANET from the attackers.

4.1. Security mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

4.1.1. Preventive mechanism: The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, pass phrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory,in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

4.1.2. Reactive mechanism: An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

4.2. Countermeasures on Network Layer Attacks

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack. IPSec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source rout etc.

The passive attack on routing information can be countered with the same methods that protect data traffic. Someactive attacks, such as illegal modification of routing messages, can be prevented by mechanisms source authentication and message integrity. DoS attacks on a routing protocol could take many forms. DoS attacks can be limited by preventing the attacker from inserting routing loops, enforcing the maximum route length that a packet should travel, or using some other active approaches. The wormhole attack can be detected by an unalterable and independent physical metric, such as time delay or geographical location. For example, packet leashes are used to combat wormhole attacks.

In general, some kind of authentication and integrity mechanism, either the hop-by-hop or the end-to-end approach, is used to ensure the correctness of routing information. For instance, digital signature, one-way hash function, hash chain, message authentication code (MAC), and hashed message authentication code (HMAC) are widely used for this purpose. IPsec and ESP are standards of security protocols on the network layer used in the Internet that could also be used in MANET, in certain circumstances, to provide network layer data packet authentication, and a certain level of confidentiality; in addition, some protocols are designed to defend against selfish nodes, which intend to save resources and avoid network cooperation. Some secure routing protocols have been proposed in MANET in recent papers. We outline those defense techniques at below sections.

4.3. Countermeasures for wormhole attacks.

A packet leash protocol is designed as a countermeasure to the wormhole attack. The SECTOR mechanism is proposed to detect wormholes without the need of clock synchronization. Directional antennas are also proposed to prevent wormhole attacks. In the wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. To defend against wormhole attacks, some efforts have been put into hardware design and signal processing techniques. If data bits are transferred in some special modulating method known only to the neighbor nodes, they are resistant to closed wormholes. Another potential solution is to integrate the prevention methods into intrusion detection systems. However, it is difficult to isolate the attacker with a software-only

approach, since the packets sent by the wormhole are identical to the packets sent by legitimate nodes. Packet leashes are proposed to detect wormhole attacks. A leash is the information added into a packet to restrict its transmission distance. A temporal packet leash sets a bound on the lifetime of a packet, which adds a constraint to its travel distance. A sender includes the transmission time and location in the message. The receiver checks whether the packet has traveled the distance between the sender and itself within the time frame between its reception and transmission. Temporal packet leashes require tightly synchronized clocks and precise location knowledge. In geographical leashes, location information and loosely synchronized clocks together verify the neighbor relation. The SECTOR mechanism is based primarily on distance-bounding techniques, one-way hash chains, and the Merkle hash tree. SECTOR can be used to prevent wormhole attacks in MANET without requiring any clock synchronization or location information. SECTOR can also be used to help secure routing protocols in MANET using last encounters, and to help detect cheating by means of topology tracking. Directional antennas are also proposed as a countermeasure against wormhole attacks. This approach does not require either location information or clock synchronization, and is more efficient with energy.

4.4. Countermeasures for black hole attacks.

Some secure routing protocols, such as the security-aware ad hoc routing protocol (SAR), can be used to defend against black hole attacks. The security-aware ad hoc routing protocol is based on on-demand protocols, such as AODV or DSR. In SAR, a security metric is added into the RREQ packet, and a different route discovery procedure is used. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. At intermediate nodes, if the security metric or trust level is satisfied, the node will process the RREQ packet, and it will propagate to its neighbors using controlled flooding. Otherwise, the RREQ is dropped. If an end-to-end path with the required security attributes can be found, the destination will generate a RREP packet with the specific security metric. If the destination node fails to find a route with the required security metric or trust level, it sends a notification to the sender and allows the sender to adjust the security level in order to find a route. To implement SAR, it is necessary to bind the identity of a user with an associated trust level. To prevent identity theft, stronger access control mechanisms such as authentication and authorization are required. In SAR, a simple shared secret is used to generate a symmetric encryption/decryption key per trust level. Packets are encrypted using the key associated with the trust level; nodes belonging to different levels cannot read the RREQ or RREP packets. It is assumed that an outsider cannot obtain the key.

In SAR, a malicious node that interrupts the flow of packets by altering the security metric to a higher or lower level cannot cause serious damage because the legitimate intermediate or destination node is supposed to drop the packet, and the attacker is not able to decrypt the packet. SAR provides a suite of cryptographic techniques, such as digital signature and encryption, which can be incorporated on a need-to-use basis to prevent modification.

V. CONCLUSION

Thus Ad-hoc networks are prove to various kinds of vulnerable attacks since they are dynamic, wireless and infrastructure less network. Besides all these hazards there are the presence of security routing protocols which make them more secure and error-free networks there by admiring the ultimate aim of Ad-hoc networks that is the accomplishment of instant network regardless of the types of nodes or type of environments that is prevailing which is described in this Paper. Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this paper, I have overviewed the challenges and solutions of the security threats in mobile ad hoc networks and study about ‘what are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?’ In our study, we classified a variety of attacks related to different layers and found that network layer is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. An answer to ‘How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?’ is that security services can be achieved through following the preventive and reactive countermeasures on the basis of particular attack. We have also described about ‘what are the countermeasures for each types of attacks in Network Layer? We focus on the potential countermeasures currently used and designed specifically for MANET. In addition, we can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. Everyday, the attackers are trying to find out the new vulnerability in MANET.

Ad Hoc networks need very specialized security methods. There is no approach fitting all networks, because the nodes can be any devices. The computer security in the nodes depends on the type of node, and no assumptions on Security can be made.

REFERENCES

[1]. Qing ting Wei, Hongzou. "Efficiency Evaluation & Comparison of Routing Protocols in MANETs" in International Symposium on Information Science & Engineering 2008.

[2]. Hongmei Deng, Wei Li, Dharma P. Agarwal, "Routing Security in Wireless Ad-Hoc Networks" in IEEE Communication Magazine Oct. 2002.

[3]. Sudip Das, "Security issues in Mobile Ad-Hoc networks"

[4]. Tarek Sheltami & Hussein Mouftah, "A Comparative study Of On-Demand & Cluster –Based Routing Protocols in MANETs", in IEEE 2003.

[5]. Williams Schilling, "Internet Protocols and Networking.

[6]. Jun Liu, Jiejun Kong, Xiaoyan Hong, Mario Gerla. "Performance Evaluation Of Anonymous Routing Protocols In MANETs"

[7]. Kaman his Biswas, Mohd. Liakat Ali. "Security Threats in Mobile Ad-Hoc Networks".

[8]. Jiangyi Hu, "Network Layer Security of Mobile Ad-Hoc Networks".

[9]. Piyush Patidar, "Mobile Ad-Hoc Networks".

[10]. Donatas Sumyla, "Mobile Ad-Hoc Networks".

[11]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile AdHoc Networks".

[12]. Prof. Deshpande Vivek S, "Security in Ad-Hoc Routing Protocols".

[13]. Rashid Hafeez Khokhar, Mohd. Asri Ngadi, Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks