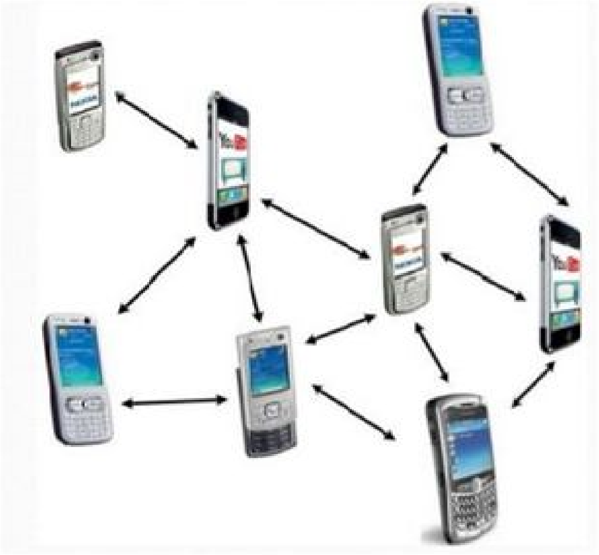
Secured Routing Mechanism in Mobile Adhoc Networks

Dr. A. Kamatchi
Associate Professor, Dept of Bachelor of Computer Application
VLB Janakiammal College of Arts and Science, Coimbatore India

Abstract- *A Mobile ad hoc network consists of a collection of autonomous wireless mobile nodes that are able to communicate with each other without the use of a network infrastructure or any centralized administration. Routing in mobile ad hoc networks faces additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. There are several well-known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth, and high error rates . Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks: the table-driven or proactive and the source-initiated on-demand or reactive approaches. This paper analyzes various routing security techniques in mobile adhoc network. It provides significant result to find secure routing technique in mobile adhoc network.*

Keywords- Mobile Adhoc Network, MANET Routing, security in Routing

I. INTRODUCTION



MANET Architecture

MANET has no fixed infrastructure. It uses dynamic changing topology. In this architecture Mobile devices join/leave the network unexpectedly and they can also move freely. MANET is energy constrained [1]. The bandwidth is very limited. Each node also serves as router in this MANET architecture. It helps to relay packets received from neighbors. It contains interoperation with the Internet. In wired networks, routers perform routing task. Special node known as access point (AP) in used in managed wireless networks.

The provision of security services in MANET is dependent on the characteristics of the supported application and the networked environment, which may vary significantly. The common assumption that MN credentials (e.g., certificates) are bound to IP addresses may need to be revisited, because one can imagine that roaming MNs will joint MANET sub domains and IP addresses will be assigned dynamically.

II. SECURITY REQUIREMENTS IN MANETS

In mobile ad hoc networks, security depends on several parameters (authentication, Confidentiality, integrity, non-repudiation and availability) [2]. Without one of these parameters, security will not be complete. Without authentication, an attacker could masquerade a node, thus being able to have unauthorized access to the resources and to sensitive information.

i) Authentication

Authentication enables a MN to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

ii) Non-Repudiation

It ensures that the original message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised MNs. Ensures that sending and receiving parties can never deny ever sending or receiving the message

iii) Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality.

iv) Key And Trust Management

Key and trust management is a critical supporting element in any security systems. Its basic operations include establishing key exchange and update, as well as secret connections. Keys are the basic blocks of symmetric and asymmetric cryptographic functions, which in turn furnish authentication, confidentiality, integrity, and non-repudiation security services

v) Availability

Availability of a network means that the network should be available to provide its services when needed even with the existence of break-ins. While survivability implies the ability of the network to provide its services under any conditions and return the service to normal levels at normal conditions. These requirements are especially important in MANETs where break-ins, attacks and malfunctions are more frequent and less detectable.

vi) Data Integrity:

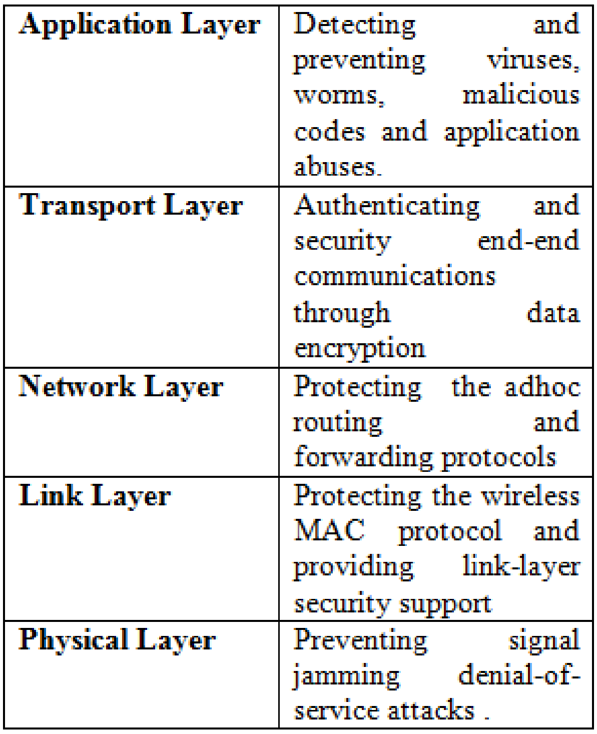
When data is exchanged between network nodes, users need to be sure that it has not been tampered with or changed on transit. This is essential in situations such as banking, military operations and equipment controls where such changes could cause potential damage[3].

vii) Access Control

Access control consists of the means to govern the way the users or virtual users such as operating system processes (subjects) can have accesses to data (objects). In networking, access control can e.g. involve the mechanisms with which the formation of groups of nodes is controlled. Only authorized nodes may form, destroy, join or leave groups. Access control can also mean the way the nodes log into the networking system to be able to communicate with other nodes when initially entering the network[4].

III. SECURITY ISSUES

i) Attacks in various Layers.



Application Layer	Detecting and preventing viruses, worms, malicious codes and application abuses.
Transport Layer	Authenticating and security end-end communications through data encryption
Network Layer	Protecting the adhoc routing and forwarding protocols
Link Layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical Layer	Preventing signal jamming denial-of-service attacks .

ii) Security Attacks against Routing in MANETs

Attacks on Routing in MANETs

To develop a good and secure routing protocol, one needs to understand the possible type of attacks on routing protocols. Below, we explain some attacks designed to disrupt routing protocols in MANETs.

Routing Loop

An attacker sends forged routing packets causing data packets to traverse nodes in a cyclical path without reaching their destinations. This attack consumes energy and bandwidth in addition to causing data packets loss [5].

Blackhole Attack

In this attack, a malicious node responds to a route request packet claiming that it has a valid and fresh route to the destination node. In this case, an attacker could trick a sender into routing all data packets to the attacker which discards them.

Grayhole Attack

It is a special case of a blackhole attack where an attacker could create a gray hole where it selectively drops some control and/or data packets. For example, forwarding some data packets and all control packets or forwarding all control packets but not data packets [6].

Blackmail Attack

In MANETs, nodes can keep track of perceived malicious nodes in a blacklist at each node, similar to watchdog and pathrater [7]. An attacker could blackmail (report) a good node, telling other nodes to add that legitimate node to their blacklists. This attack results in isolating legitimate nodes from the network.

Gratuitous Detour Attack

An attacker may also attempt to cause a node to use detours (suboptimal routes) or may attempt to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another. An attacker may attempt to make a route through itself appear longer by adding virtual nodes to the route [8].

iii) Types of security attack in MANET Routing.

Security attacks in MANET routing can be divided in two main types, passive attacks and active attacks. The intention of a passive attack is typically to listen and retrieve vital information inside data packets, for example by launching a traffic monitoring attack. In such an attack, a malicious node tries to identify communication parties and functionality which can provide information to launch further attacks. The attack type is called passive since the normal functionality of the network is not altered.

An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET[9].

- Modification attacks
- Impersonation attacks
- Fabrication attacks
- Wormhole attacks
- Selfish behavior.

Modification Attacks

A modification attack is typically launched by a malicious node with the deliberate intention of redirecting routing packets, by for example modifying the hop count value of a routing packet to a smaller value. By decreasing the hop count value a malicious node can attract more network communication. A typical modification attack is the black hole attack where a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. As a result, the target node will send its packets through the malicious node when communicating with the destination node. The malicious node can choose to either drop the packets or place itself on the route as the first step in what is known popularly as either the manin- the-middle (MITM) or a SYBIL attack.

Impersonation/Spoofing Attacks

In this type of attack (also known as spoofing) a malicious node uses for example the IP or address of another node in outgoing routing packets. As a result, the malicious node can receive packets meant for the other node or even completely isolate it from the network.

Fabrication

The main purpose of fabrication attacks is to drain off limited resources in other MANET nodes, such as battery power and network connectivity by, for example, flooding a specific node with unnecessary routing messages. A malicious node can for example send out false route error messages.

A fabrication attack can also be launched by a selfish node that duplicates the transmission of packets to another node, just to make sure all packets will reach the destination node. This behavior may lead to an excessively high network traffic load.

Wormhole Attacks

A wormhole is a particularly severe attack on MANET routing. A malicious node captures packets from one location in a network and tunnels them to another malicious node, located several hops away, which forwards the packets to its neighboring nodes. This creates the illusion that two endpoints of a wormhole tunnel are neighbors even though they are located far away from each other in reality. A strategic placement of a wormhole causes most of the network traffic to pass through the malicious nodes which have formed the wormhole. Once the wormhole link has been successfully established, further attacks can be launched by the malicious nodes such as selective packet drop to disrupt communication or data sniffing to capture confidential information.

Selfish Behavior

This refers to a node which does not cooperate in any routing. It may for example, be that it wishes to save energy and so switches to a “sleep mode” whenever it is not taking part in any network communication. While such an attack may not be launched with explicitly bad intentions, it can lead to serious disruptions in network communications such as high route discovery delays and dropped data packets. If the selfish node also happens to be the only communication link between two MANET endpoints, communications between these endpoints will become unavailable.

IV. SECURE ROUTING PROTOCOLS

i) Security Aware Ad hoc Routing (SAR)

The SAR protocol incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key[10].

ii) Authenticated Routing for Ad hoc Networks (ARAN)

The purpose of the ARAN protocol is to detect and protect against malicious actions by third parties and peers. It provides authentication, message integrity, and nonrepudiation. ARAN can be used in two different security stages: a simple mode which is mandatory and an optional stage which provides stronger security but also more overhead and is not suitable on mobile devices with very low processing or battery capacity. ARAN uses cryptographic certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbors. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own[11].

iii) Secure Efficient Ad hoc Networks (SEAD)

SEAD is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update message is verified by a receiving node. Looping is removed by using a sequence number and authentication of the source of routing update message. Authentication of the source can be done for example by providing a shared secret key between each pair of nodes in the MANET which is then used for MAC calculations between the nodes for the authentication of a routing update message[12].

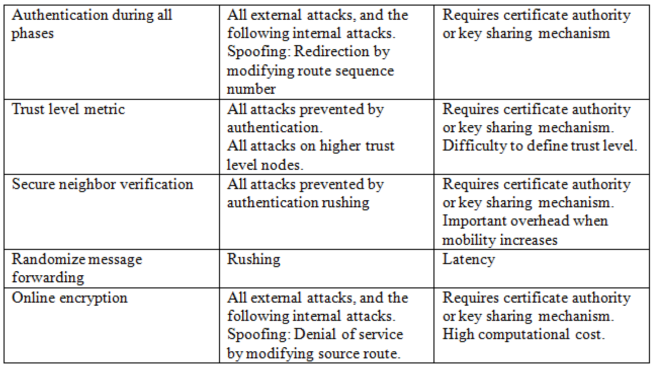
iv) Secure Link State Routing Protocol (SLSP)

The main functionality of SLSP is to secure the discovery and the distribution of link state information by using asymmetric keys. SLSP consists of three major steps: public key distribution, neighbor discovery, and link state updates. Public keys are distributed between a node and all its neighbors. A central server for key distribution is thus not needed[13].

v) Secure Routing Protocol (SRP)

SRP is a protocol designed to secure ZRP but can also be used with pure reactive routing protocols. A security association (SA) is required between a source node and a destination node. It is assumed that the SA can be established by using a shared key between the two communicating nodes. SRP uses an additional header to the underlying on-demand routing protocol packet. The header contains a sequence number QSEC, an ID number QID, and a MAC field where the output of a key hashed functions is inserted. A route request messages is discarded by intermediate nodes if the SRP header is missing[14].

V. SOLUTIONS TO SECURE ROUTING PROTOCOLS



Authentication during all phases	All external attacks, and the following internal attacks. Spoofing: Redirection by modifying route sequence number	Requires certificate authority or key sharing mechanism
Trust level metric	All attacks prevented by authentication. All attacks on higher trust level nodes.	Requires certificate authority or key sharing mechanism. Difficulty to define trust level.
Secure neighbor verification	All attacks prevented by authentication rushing	Requires certificate authority or key sharing mechanism. Important overhead when mobility increases
Randomize message forwarding	Rushing	Latency
Online encryption	All external attacks, and the following internal attacks. Spoofing: Denial of service by modifying source route.	Requires certificate authority or key sharing mechanism. High computational cost.

VI. CONCLUSION

In this paper we discussed the security issues in MANETs at the network layer. To provide a good understanding of the issues, we started with a general overview of the network security, mobile wireless networks and the security requirements for MANETs. The study focused on the network layer and the security of the routing protocols. Due to the fact that many of the security protocols realized at the higher levels assume secure and robust routing in the network. In addition, the security protocols at the transport and application layers share the same general principles in regular, wireless and adhoc networks. However, unlike in regular networks, where specially designed routers and switches are used. MANET devices have to perform the task for each other. This creates the possibility of having selfish and misbehaving nodes in addition to compromised and impersonated nodes. To ensure the correct operations of the MANET, it is essential to have correct and secure routing mechanism.

REFERENCES

[1] Abusalah, L., Khokhar, A., & Guizani, M. “A Survey of Secure Mobile Ad Hoc Routing Protocols”. IEEE Communications Surveys & Tutorial, 10 (4), 78-93, 2008.

[2] Basagni .S, Herrin .K, Rosti .E, and Bruschi .D, “Secure Pebble nets, in: Proceedings of 2nd MobiHoc”, Long Beach CA, pp.156–163, October 2001.

[3] Boukerche .A, El-Khatib .K, Xu .L,Korba .L, “Secure ad hoc routing protocol”, Fourth International IEEE Workshop on Wireless Local Networks. Tampa, Florida, November 2004. NRC47394, 2004.

[4] Buchegger, S., & Boudec, J.-Y.L. “Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks”. Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC) 2002.

[5] Chang YF, Chang CC, Liu YL. “Password authentication without the server public key”. IEICE Transactions on Communications; E87-B(10): 3088–3091, 2004.

[6] DeCleene B, Dondeti L, Griffin S, et al “Secure communications for wireless networks”. IEEE MILCOM. Communications for Network-Centric Operations: Creating the Information Force; 1: 113–117,2001.

[7] Garg, N. & Mahapatra, R.P. “MANET Security Issues”. IJCSNS International Journal of Computer Science and Network Security, 9 (8), 2009.

[8] Goyal, T., Batra, S. & Singh, A. “A Literature Review of Security Attack in Mobile Ad-hoc Networks”. International Journal of Computer Applications, 9 (12), 11-15, 2010.

[9] Pearlman .M. R, Haas .Z .J, Sholander .P, Tabrizi S. S, “On the impact of alternate path routing for load balancing in mobile ad hoc networks”, Mobi HOC, 2000.

[10] Luo .H, Zerfos .P, Kong .J, Lu .S, and Zhang .L, “Self-securing adhoc wireless networks”, Proceedings of the IEEE International Symposiumon Computers and Communications (ISCC), Taormina, Italy, 2000.

[11] Perkins C. DSDV: routing over a multihop wireless network of mobile computers. In Ad hoc Networking. Addison-Wesley: Reading, MA, 2001.

[12] Perrig .A, Szewczyk .R, Wen .V, Culler .D, and Tygar J.D, “SPINS: security protocols for sensor networks”: Proceedings of the 7th Annual International Conference in Mobile Computing and Networks (MobiCom 2001), Rome, Italy, pp. 189–199, 2001.

[13] Varadharajan V, Shankaran R, Hitchens M. “Security for cluster based ad hoc networks. Computer Communications” , 27: 488–501, 2004.

[14] Vassilaras S, Vogiatzis D, Yovanof GS. Security and cooperation in clustered mobile ad hoc networks with centralized supervision. IEEE Journal on Selected Areas in Communications, 24(2): 329–342, 2006.