ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Security Issues in Wireless Ad-Hoc Network Routing Protocols

[I]S.Venkata Lakshmi, [II]D. Kusumalatha
[I,II]Dept. of CSE, KMM Engineering College, Tirupathi, India
[I]sibbalalakshmi@gmail.com, [II]kusumalatha.dasari@gmail.com

Abstract
An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. Due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and presents a number of challenges in ensuring the security of the communication. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. We first analyze the main Vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. The general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation treating as equally and absence of traffic diversion.

Keywords
Routing, Security Attacks, Wireless Networks

I. Introduction

A Mobile Ad-Hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

Operating in ad-hoc mode allows all wireless devices within the range of each other to discover and communicate in peer-to-peer fashion without involving central access. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wire Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching.

The wireless nature of communication and lack of any security infrastructure raises several security problems. Figure 1 shows the working of ad hoc network. There are two different types of wireless networks. The first and easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range.

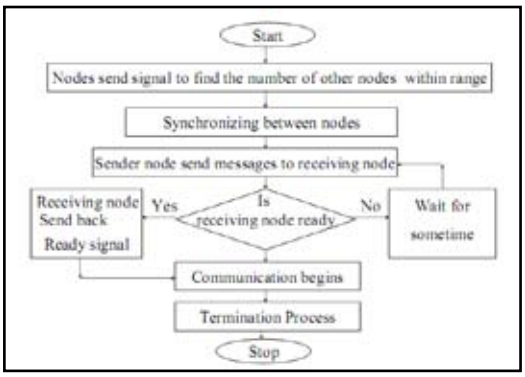

Fig. 1: Working of a General Ad-Hoc Network

The mobile ad hoc network has the following typical features:

- Unreliability of wireless links between nodes.
- Constantly changing topology.
- Lack of incorporation of security features.

1. Security Issues

Security is an important issue for wireless networks, especially for those security sensitive applications. Many users of data transmission devices (such as laptops, PDAs, PCs, phones, etc.) demand for Protecting data residing within devices, protecting the transmission network, protecting transfer of data, and ensuring proper transfer. One of the goals of current wireless standard was to provide security and privacy that was 'Wired equivalent' and to meet this goal, several security mechanism were provided for confidentiality, authentication, and access control. Unfortunately all of these can be easily broken. Points to consider as security parameters are:

1. Identity: An essential element in any security system is reliable, robust non-malleable identity.
2. Access control: Access control is the constraint that limits those who can utilize system resources. Two approaches are used, one is called 'access control list (ACL)' and other as 'closed network'.
3. Authentication: It ensures that communication from one node to other is genuine. Only legitimate users can access the system and services. Two used systems are 'open system' and 'shared key'.
4. Availability: Availability ensures the service offered by node will be available to its users when expected, in spite of attacks. Also only legitimate users can access data anytime.
5. Integrity: It protects nodes from maliciously altered messages. The receiver wants to be sure that the source is genuine. It assures the data, system or platform has not been tampered with.
6. Non repudiation: It ensures that the origin of the message cannot deny having sent the message.
7. Confidentiality: It ensures that certain information is never disclosed to unauthorized entities. Personal or sensitive data is protected.

2. Attacks

There are two types of attacks toward security protocols: (a)

External and (b) Internal.

II. Routing Protocols Security Issues

The occurring routing protocols for Ad-Hoc networks deal effectively with something difficulty well with dynamically changing topology but are not designed to accommodate defense against intending attackers. Today's routing algorithms are not able to prevent from common security threats. Threats and attacks against ad hoc routing under several areas of application and suggested solutions that could be used when secure protocols are designed.

A. Types of Ad-Hoc Routing Protocols

Ad hoc network is a multi hop wireless network, which consists of number of mobile nodes. These nodes generate traffic to be forwarded to some other nodes or a group of nodes. Due to a dynamic nature of ad hoc networks, traditional fixed network routing protocols are not viable. Based on that reason several proposals for routing protocols have been presented.

In general there are two types of routing protocols: Proactive and Reactive routing protocols. In Proactive Routing Protocols, the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and the Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF). In Reactive or On Demand Routing Protocols the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV).

In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology.

B. Types of Attacks Faced by Routing Protocols

Attacks arising from malicious behavior can be divided in to those where packets are originated by the malicious node and those where a malicious node is an intermediate node and receives control packets for forwarding. When a malicious node is originating packets, it can send control packets using its own source address, an address which belongs to an existing node in the ad hoc network, or an arbitrary address which does not belong to any node. Malicious intermediate nodes can either modify or replay received packets.

The relevant attack methods are:

- Masquerading as an existing node,
- Masquerading as a previously connected node,
- Replay attacks,
- Byzantine behavior to attract traffic,
- Byzantine behavior to deflect traffic, and
- Misdirection using a wormhole.

Conventionally, origin authentication mechanisms are needed to prevent masquerade attacks. In this we first analyze the inherent security of proactive and reactive protocols when origin authentication is not used for internal nodes, or when a malicious node has found a way to circumvent the mechanisms used for origin authentication. This can be achieved by sending false control packets using an incorrect source address; this address could either belong to a node currently routing in the network, or it could be an address which is not currently being used, perhaps of a node which was previously connected to the ad hoc network. Such false control packets are also referred to as spoofed packets. Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network. The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. An Active Attack, however, 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 goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

C. Attacks Against Ad-Hoc Routing Networks

While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the very nature of radio transmissions, which are made on the air. The most prominent (important) attacks prevalent against ad hoc networks, most of which are active attacks.

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/ delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack.

- Impersonating another node to spoof route message. Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack. Modifying a Route Reply message to inject a false route.
- Generating bogus Route Error to disrupt a working route. Suppressing Route Error to mislead others.

Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages. There are some more sophisticated routing attacks, which include Wormhole attacks, Rushing attacks and Sybil attacks.

The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented. There are two main attack strategies in this 10 type: one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save it own battery power; the other is denial-of-service.

1. Attacks Based on Modification

This is the simplest way for a malicious node to disturb the operations of an ad-hoc network. The only task the malicious node needs to perform, is to announce better routes (to reach other

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

nodes or just a specific one) than the ones presently existing. This kind of attack is based on the modification of the metric value for a route or by altering control message fields.

There are 3 ways in which this can be achieved: Redirection by Changing the Route Sequence Number: When deciding upon the best / optimum path to take through a network, the node always relies on a metric of values, such as hop count delays etc. The smaller that value, the more optimum the path. Hence, a simple way to attack a network is to change this value with a smaller number than the last "better" value. Redirection by Altering the Hop Count: This attack is more specific to the AODV protocol wherein the optimum path is chosen by the hop count metric.

In general, an attacker would use a value zero to ensure to the smallest hop count. Taking for example the 'wormhole' attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them there into the network. This could potentially lead to a situation where, it would not be possible to find routes longer than one or two hops, probably disrupting communication. Denial of Service by Altering Routing Information: Consider, in a bus topology, a scenario wherein a node A wants to communicate with node E. At node A the routing path in the header would be A-B-C-D-E. If B is a Compromised node, it can alter this routing detail to A-B-C-E. But since there exists no direct route from C to E, C will drop the packet.

Thus, A will never be able to access any service / information from E. Another instance can be seen when considering a category of attacks called 'The Black Hole Attacks'. It can then choose to drop the packets thereby creating DoS.

2. Impersonation Attacks

More generally known as 'spoofing', since the malicious node hides its' IP and or MAC address and uses that of another node. Since 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. Take for example a situation where in an attacker creates loops in the network to isolate a node from the remainder of the network. To do this, the attacker needs to spoof the IP address of the node he wants to isolate from the network and then announce new route to the others nodes. By doing this, he can easily modify the network topology as he wants.

3. Attacks by Fabrication of Information

There are basically 3 sub categories for fabrication attacks.

In any of the 3 cases, detection is very difficult. Falsification of Rote Error Messages: This attack is very prominent in AODV and DSR, because these two protocols use path maintenance to recover the optimum path when nodes move. The weakness of this architecture is that whenever a node moves, the closest node sends an "error" message to the other nodes so as to inform them that a route is no longer accessible. If an attacker can cause a DoS attack by spoofing any node and sending error messages to the all other nodes. Thus, the malicious node can isolate any node quite easily. Corrupting Routing State - Route Cache Poisoning: A passive attack that can occur especially in DSR due to the promiscuous mode of updating routing tables which is employed. This occurs when information stored in routing tables is deleted, altered or injected with false information. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination.

If enough routes are created, new routes can no longer be added due to an overwhelming pressure on the protocol. After considering all the above plausible attacks we can draw a conclusion that we need to have a routing protocol that establishes routes without being susceptible to false information from any malicious node. A good routing protocol should also be able to detect the malicious nodes and to react in consequence, by changing routes, etc.

III. Components of Wireless Networks

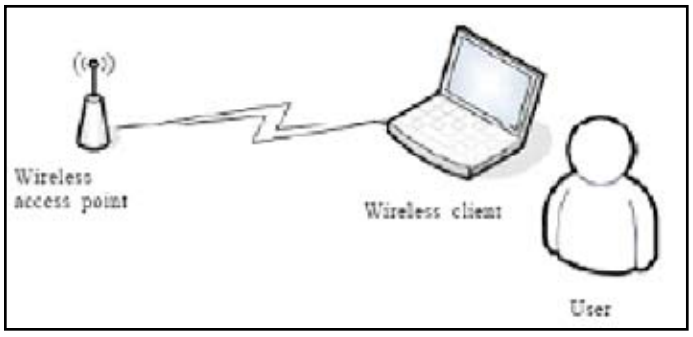

Fig. 2: Wireless Networking Components

IV. Classification Techniques

In order to provide solutions to the security issues involved in ad-hoc networks, we must elaborate on the two of the most commonly used approaches in use today:

- Prevention
- Detection and Reaction

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals.

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing o forward packets and then failing to do so, because it is overloaded, selfish or malicious. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets.

A malicious node launches a denial of service attack by dropping packets. All protocols defined in this category detect and react to such misbehavior. Using this as the basis for our survey, we describe the following broad classifications:

1. Prevention using asymmetric cryptography
   - Using symmetric cryptography
   - Using one-way hash chains
2. Detection and Reaction

V. Reasons for Wireless Network Usage

1. Mobility: Information access beyond the desk.
2. Simplicity: Elimination of the needs for complex cabling and construction.
3. Flexibility: Being well suited for too many environments.
4. Accessibility: Being available at airports, hotels,coffee shops and convention centers are just a few places where hot-spot access.

VI. Applications of Ad-Hoc Wireless Networks

- Military applications
- Collaborative and Distributed Computing
- Emergency Operations

The main objective of the protocol is to avoid any malicious node from falsely advertising a better route or tamper the sequence number in the packet that it received from the source. They basically implement features to protect modification of routing information such as metric, sequence number and source route. SEAD uses a one-way hash chains for authenticating the metric and the sequence number. Each node creates a one-way hash chain and uses the elements in groups of 'm' (given m as the diameter of the network) for each sequence number. Each node uses a specific single next element from its hash chain in each routing update that it sends about itself (metric 0). The upper bound of the network is denoted by (m-1).

An entry is authenticated by using the sequence number in that entry to determine a contiguous group of m elements from that destination node's hash chain, one element of which must be used to authenticate that routing update. The one-way nature of hash chains prevents any node from advertising a route with a greater sequence number than the source's sequence number.

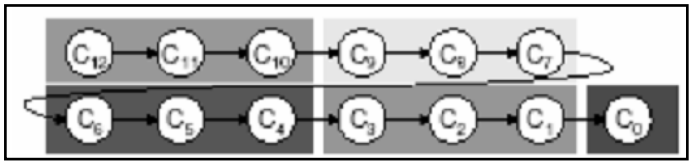

Fig. 3: Hash Chains in SEAD

To avoid routing loops the source of each routing update message must be authenticated. This protocol requires pair wise shared secret keys or broadcast authentication such as TESLA, HORS or TIK to authenticate neighbors.

Which include modification/ fabrication of packets, dropping packets, among others, caused by selfish or malicious nodes, collectively known as Byzantine failures.

Three primary differences from Fail-Stop Failure:

1. Component can produce arbitrary output
• Fail-stop: produces correct output or none.
2. Cannot always detect output is faulty
• Fail-stop: can always detect that component has stopped.
3. Components may work together maliciously.

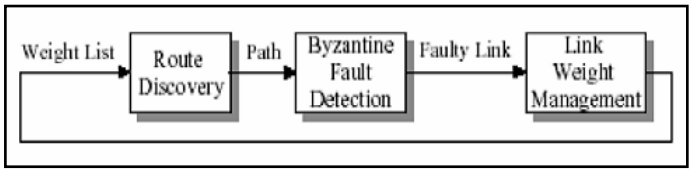

Fig. 4: Phases of Byzantine Algorithm

The above figure depicts the 3 phases of the Byzantine algorithm, i.e. Link Weight Management, Route Discovery with Fault Avoidance, and Byzantine Fault Detection.

Byzantine Agreement is a kind of guaranteed multicast of a value in which one process sends its value (bit) to other participants and they exchange various messages in order to agree on exactly what value was sent. It results when all correctly operating processes are able to agree either on a value or on the conclusion that the originator of the value is faulty. It is called Byzantine because we make no assumption about the behavior of any undetected faulty processes. More explicitly, Byzantine Agreement is achieved when

1. All correctly operating processes agree on the same value, and
2. If the transmitter operates correctly, then all correctly operating processes agree on its value. Implicit in (I) and (II) is the idea that the agreement is synchronous in the sense that all processes reach this agreement at the same time.

The objective of Byzantine fault tolerance is to be able to defend against Byzantine failures, in which components of a system fail in arbitrary ways (i.e., not just by stopping or crashing but by processing requests incorrectly, corrupting their local state, and/or producing incorrect or inconsistent outputs.). Correctly functioning components of a Byzantine fault tolerant system will be able to correctly provide the system's service assuming there are not too many Byzantine faulty components.

VII. Conclusion

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently.

Self-organization is a key property of ad-hoc networks. Besides authentication, confidentiality, integrity, availability, access control, and non repudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion. The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior, preventing someone else from getting proper service, extracting data to get confidential information, and so on.

Routes should be advertised and set up adhering to the routing protocol chosen and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network. We have discussed the various routing and forwarding attacks in this survey. We have also discussed prevention and detection mechanisms that were adopted to provide security in ad hoc networks.

A prevention-only strategy will only work if the prevention mechanisms are perfect; otherwise, someone will find out how to get around them. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. In view of this reality, detection and response are essential. In this paper we discussed proposals representing all of these classes. Even though prevention works as the first line of defense, it is not sufficient in addressing all the security threats. Hence we suggest an integrated layered framework which adopts the prevention techniques for the first level and detection techniques can be used at the second level complementing the protection techniques.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

References

[1] *J.-P. Hubaux, L. Buttyan, S. Capkun,"The quest for security in mobile ad hoc networks", In The 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing, October 2001.*

[2] *L. Zhou, Z. Haas,"Securing Ad-Hoc networks", IEEE Network Magazine, Vol. 13, November/December 1999.*

[3] *Manel Guerrero Zapata,"Secure Ad-Hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt, August 2002. First published in the IETF MANET Mailing List (October 8th 2001).*

[4] *Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields,"A Secure Routing Protocol for Ad-Hoc Networks", In Proceedings of the 10 Conference on Network Protocols (ICNP), November 2002.*

[5] *S. Yi, P. Naldurg, R. Kravets,"Security-Aware Ad hoc routing for Wireless Networks The Second ACM Symposium on Mobile Ad-Hoc Networking & Computing (MobiHoc'01), 2001.(another version Security-Aware Ad-Hoc Routing Protocol for Wireless Networks, Report, August, 2001).*

[6] *Panagiotis Papadimitratos, Zygmunt J. Haas,"Secure Routing for Mobile Ad-Hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.*

[7] *Yih-Chun Hu, David B. Johnson, Adrian Perrig,"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad- Hoc Networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.*

[8] *Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, Herbert Rubens,"An On-Demand Secure Routing Protocol Resilent to Byzantine Failures", In ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, September 28 2002.*

[9] *Pietro Michiardi, Refik Molva Core,"A Collaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security 2002 Conference.*