IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 7, Jul 2014, 105-112
© Impact Journals

SECURITY THREATS AND PREVENTIONS IN MOBILE AD-HOC NETWORK (MANET)

MD. IMRAN HOSSAIN

Department of Information & Communication Technology, Comilla University, Comilla, Bangladesh

ABSTRACT

A mobile ad-hoc network (MANET) is a self-configuring network consists of mobile routers (included associated hosts) connected by wireless links which build a capricious topology forms the union. The routers are free to move randomly and organize themselves at a random manner; as a result, the network's wireless topology could change rapidly and unpredictably. MANETs are usually used in the situations of urgency for temporary operations or simply if there are no resources to set up sophisticated networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to set up, at the same time however, due to the absence of any fixed structure, it becomes difficult to make use of the existing routing techniques for network services. At this circumstance it poses a number of challenges for the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices those has the properties like low power consumption, low processing load etc. Many of the ad hoc routing protocols that address security issues rely on inherent trust relationships to route packets among participating nodes. Besides the general security issues like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation equality and absence of traffic diversion. In this Paper the security issues of MANETs are emphasized in concern of different aspects.

KEYWORDS: MANET, Topology, Infrastructure, Power Consumption, Protocol, Authentication, Confidentiality, Integrity, Non-Repudiation

INTRODUCTION

Ad-hoc networks are a new archetype of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other’s radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Mobility of the nodes causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure causes several security problems. The current security of the ad-hoc network is dependent on the algorithm based security. The focus is mainly on the security of the routing protocols used in the second kind of ad-hoc network described above. Any routing protocol must summarize an essential set of security concern. These are mechanisms that help to prevent, detect, and respond to different types of attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

- **Secrecy:** In ad-hoc networks secrecy is more difficult to achieve because intermediate nodes (that act as routers) receive the packets for other recipients, so they can easily snoop the information being routed.

- **Ease of Use:** Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer intruder can use jamming techniques to interfere with communication on physical channel. On network layer the intruder can disrupt the routing protocol. On higher layers, the intruder could bring down high level services e.g. key management service.
- **Authentication:** Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would imitate a node, thus gaining illegal access to resource and sensitive information and interfering with operation of other nodes.
- **Integrity:** Message that is transmitted is never altered.
- **Non-Repudiation:** Ensures that sending and receiving parties can never deny ever sending or receiving the message.

All the above security mechanisms must be considered in any ad-hoc networks so as to ensure the security of the transmissions along that network.

Broadly there are two major categories of attacks when considering any network *Attacks from outside sources* and *attacks from within the network.* The second attack is more meticulous and detection and correction is difficult. Routing protocol should be able to secure themselves against both of these attacks.

In mobile ad-hoc networks, nodes do not rely on any routing infrastructure but relay packets between them. Thus communication in mobile ad-hoc networks functions properly only if the participating nodes cooperate in routing and forwarding [1] [2][3].

TYPES OF ATTACKS FACED BY ROUTING PROTOCOLS

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. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

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.

- **Attacks Based on Alteration**

This is the easiest way for a malicious node to disturb the operations of an ad-hoc network. The only task the malevolent node needs to perform, is to announce better routes (to reach other 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.*
- *Redirection by altering the Hop Count.*
- *Denial of Service by Altering Routing Information.*

- **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.

- **Attack by Fabrication of Information**

There are basically 3 sub categories for fabrication attacks. In any of the 3 cases, detection is very difficult.

- *Prevarication of Rote Error Messages.*
- *Mortifying Routing State - Route Cache Poisoning.*
- *Routing table overflow attack.*

INSIDER ATTACKS

There are some insider attacks against MANET routing protocols. These attacks could be identified as an inside attacker may desire to achieve and further classify the misuses of the AODV protocol into two categories namely atomic misuses and compound misuses.

Misuse Goals

- **Route Disruption (RD):** Breaking down an existing route or preventing a new route from being established.
- **Route Invasion (RI):** Inside attacker adds itself between two endpoints of a communication channel.
- **Node Isolation (NI):** Preventing a node from communicating with any other node.
- **Resource Consumption (RC):** Consuming network bandwidth or storage space.

In general terms, an attacker that can forward ROUTE REQUESTs more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes. This attack is also particularly damaging because it can be performed by a relatively weak attacker.

CLASSIFICATIONS OF TECHNIQUES USED TO SECURE AD-HOC NETWORKS

Prevention Using Asymmetric Cryptography: Secure Ad-Hoc on-Demand Distance Vector Routing Protocol (SAODV)

SAODV adds security to the famous AODV protocol. Its basic functionality lies in securing the ADOV protocol by authenticating the non-mutable fields of the routing message using digital signatures. It also provides an end-to-end authentication and node-to-node verification of these messages. The underlined process is relatively simple. The source node digitally signs the route request packet (RREQ) and broadcasts it to its neighbors. When an intermediate node receives a RREQ message, it first verifies the signature before creating or updating a reverse route to its predecessor.

It then stores or updates the route only if the signature is verified. A similar procedure is followed for the route reply packet (RREP). As an optimization, intermediate nodes can reply with RREP messages, if they have a “fresh enough” route to the destination. Since the intermediate node will have to digitally sign the RREP message as if it came from the destination, it uses the double signature extension described in this protocol. The only mutable field in SAODV messages is the hop-count value. In order to prevent wormhole attacks this protocol computes a hash of the hop count field [4].

Prevention Using Asymmetric Cryptography: Authenticated Routing for Ad-Hoc Networks (ARAN)

ARAN is an on-demand routing protocol that makes use of cryptographic certificates to offer routing security. Its main usage is seen in managed-open environments. It consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication.

This protocol requires the use of a trusted certificate server T, whose public key is known to all the nodes in the network. End-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet. The RDP packet contains a nonce and timestamp to prevent replay attacks and to detect looping. Similarly, each node along the reverse path (destination to source) signs the REP and appends its own certificate before forwarding the REP to the next hop [5].

Prevention Using Symmetric Cryptography: Security-Aware Ad Hoc Routing (SAR)

SAR is an attempt to use traditional shared symmetric key encryption in order to provide a higher level of security in ad-hoc networks. The SAR protocol makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Although current routing protocols discover the shortest path between two nodes, SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key). The different trust levels are implemented using shared symmetric keys. In order for a node to forward or receive a packet it first has to decrypt it and therefore it needs the required key. Any nodes not on the requested trust level will not have the key and cannot forward or read the packets. Every node sending a packet decides what trust level to use for the transfer and thereby decides the trust level required by every node that will forward the packet to its final destination.

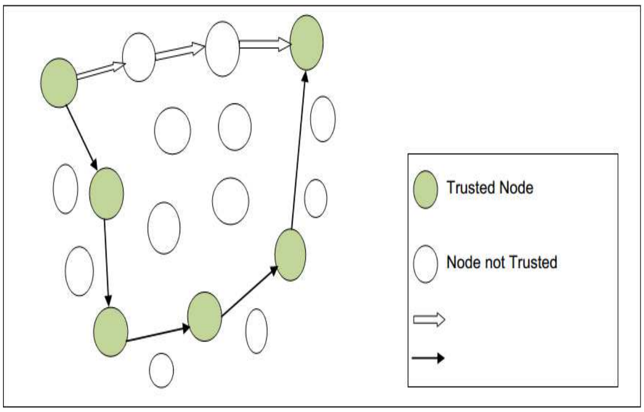

Figure 1: Variation of Shortest Path Route Selection between SAR and Other Routing Algorithms

SAR is indeed secure in the way that it does ensure that only nodes having the required trust level will read and reroute the packets being sent. Unfortunately, SAR still leaves a lot of security issues uncovered and still open for attacks such as:

- Nothing is done to prevent intervention of a possibly malicious node from being used for routing, as long as they have the required key
- If a malicious node somehow retrieves the required key the protocol has no further security measure to prevent against the attacker from bringing the entire network to a standstill.
- There is excessive encryption and decryption required at each hop. Since we are dealing with mobile environments the extra processing leading to increased power consumption can be a problem.

SAR is intended for the managed-open environment as it requires some sort of key distribution system in order to distribute the trust level keys to the correct devices [6].

Prevention Using Symmetric Cryptography: Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP), is another protocol extension that can be applied to any of the most commonly used protocols today. The basic idea of SRP is to set up a security association (SA) between the source and the destination node [10]. An SA is a secret-key scheme used to preserve integrity in the routing information. The SA is usually set up by negotiating a shared key based on the other party's public key, and after that the key can be used to encrypt and decrypt the messages. The routing path is always sent along with the packets, unencrypted though (since none of the intermediate nodes have knowledge of the shared key).

As an example we can say that the source node (S) initiates the route discovery by constructing a route request packet. The route request packet is identified by a random query identifier (rnd#) and a sequence number (sq#). We assume that a security association (a shared key K_{ST}) is established between source (S) and destination (T). S constructs a MAC such that, MAC = h(S, T, rnd#, sq#, K_{ST}). In addition the IP addresses of the traversed intermediate nodes are accumulated in the route request packet.

Intermediate nodes relay route requests. The intermediate nodes also maintain a limited amount of state information regarding relayed queries (by storing their random sequence number), so that previously seen route requests are discarded. Intermediate nodes relay route requests. The intermediate nodes also maintain a limited amount of state information regarding relayed queries (by storing their random sequence number), so that previously seen route requests are discarded.

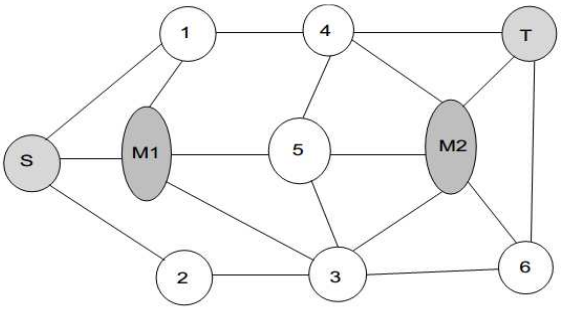

Figure 2: Sample Working of SRP

More than one route request packet reaches the destination through different routes. The destination T calculates a MAC covering the route reply contents and then returns the packet to S over the reverse route accumulated in the respective request packet. The destination responds to one or more route request packets to provide the source with an as diverse topology picture as possible [7].

Prevention Using One-Way Hash Chains: SEAD

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.

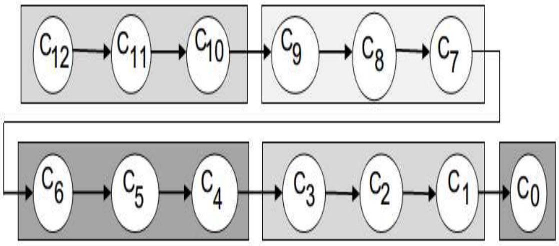

Figure 3: Hash Chains in SEAD

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 [8].

Prevention Using One-Way Hash Chains: ARIADNE

The ARIADNE protocol relies only on highly efficient symmetric cryptography. The protocol primarily discusses the use of a broadcast authentication protocol namely TESLA, because of its efficiency and requires low synchronization time rather than the high key setup overhead of using pair-wise shared keys. Other authentication protocols such as BiBa are / can also be used for this purpose [9]. This proposal is an on-demand routing protocol. The design of Ariadne can be viewed as a 3 step process:

- *Authentication of RREQ by target.*
- *Mechanisms for authenticating data in RREQ and RREP.*
- *Per-hop hashing technique.*

CONCLUSIONS

Mobile ad-hoc networks have properties that increase their susceptibility to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Self-organization is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. Latency is inherently increased in wireless multi-hop networks, depicted message exchange for security more expensive. Multiple paths are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding. 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. Prevention and detection mechanisms that were adopted to provide security in ad hoc networks are discussed. 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. Hence suggestion is given here of 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.

REFERENCES

1. J.-P. Hubaux, L. Buttyan, and 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 and Z. Haas, Securing ad hoc networks," IEEE Network Magazine, vol. 13, November/December 1999.
3. Sonja Buchegger and Jean-Yves Le Boudec. Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness In Lecture Notes on Informatics, Mobile Internet Workshop, Informatik 2002, Dortmund, Germany, October 2002. Springer.
4. 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).
5. 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.
6. S. Yi, P. Naldurg, and 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).
7. Panagiotis Papadimitratos and 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.

8. Yih-Chun Hu, David B. Johnson, and 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.

9. Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA.

10. P. Papadimitratos, Z. J. Haas, P. Samar The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routing-protocol-00.txt 2002-12-11.