SECURITY ISSUES AND ITS CHALLENGES FOR HOST BASED MOBILE AD HOC NETWORKS TO PROTECT INTRUSION

Prabhudutta Ray
rayprabhu@yahoo.com

Abstract: - Providing security to mobile ad hoc network is itself a great challenge for the researcher. Since mobile ad hoc network is highly vulnerable to face different attacks due to its self organizing behavior, infrastructure less architecture and multihop network characteristics. The strength of ad hoc network infrastructure (due to wireless and distributed nature of MANETs) also becomes the point of its greatest vulnerability. Thus decreasing the confidence level of the systems as it pertains to availability, reliability, and data integrity and privacy concern. This paper discusses some of the major security issues in terms of protocols analysis and suitability of the proposed host based intrusion detection architecture towards protecting each node from vulnerable attack.

Keywords: - MDM, ADM, DSDV, WRP, CGSR, GAR, FSR, ABR, DSR, AODV etc.

1. Introduction

wireless ad hoc networks are decentralized in nature where there is no infrastructure to inspect and manage the trafficking of information between the existing nodes and the behavior of the each node participating in the communication. However merely transferring data between nodes without safeguarding the data and preventing any corruption is not complicit with efficiency. True efficiency by default must address the incorporation of the security methods to prevent and/or reduce data breaches. Each node in the network should be strong enough to detect and protect him from any type of attack and should not be compromised with other network or do not allow any intruder in the network to capture any necessary private information. In earlier paper proposed intrusion detection architecture for each node to protect any intruder to gain control in the established ad hoc network. But some of the areas where risks are still associated with security in a wireless ad hoc network and need some practical suggestions to reduce and react to breaches. Some of the potential areas of exploration of security concerns will be like routing protocol used, encryption of confidential data for data transmission, physical security measures of the network as well as for each node and protection against attacks, etc. Mobile ad hoc networks can vary with respect to its application domain. Some application domains are emergency search and rescue operation in flood and earthquake, environmental monitoring and military applications. However depending on the use in the application domain, the hardware requirements, network configuration and resource usage / requirements will likewise vary. But certain issues are universal consideration when it comes to security [14, 15, 16].

2. Routing protocols

Due to fundamental difference in architecture ad hoc networks entails certain considerations with respect to routing protocols.

- A routing protocol should not require any centralized entity. It should be reliable enough in that each node should be able to make routing decisions based on other available participating node in that network or other networks.

- A routing protocol should be energy efficient due to limited resources like energy and computing power.

- Due to infrastructure problems ad hoc networks makes it vulnerable to security breaches. The major risk at the physical layer that leads to a denial of service, as well as need for implementing encryption and authentication in the routing protocols.
Further proactive and reactive protocols may increase network reaching ability, reliability and efficiency.

Throughput and delay can be the major concern for quality of service especially if real-time services are needed. In the earlier proposed architecture (below figure 1) there are two basic issues that are taken into consideration for routing protocols: should each node maintain a record of routes to all possible destinations or only those of immediate interest. Proposed architecture demands only those of immediate interest. In mobile ad hoc networks a node does not usually need to know a route unless it is an intermediate or the destination node [1, 6].

3. Proactive routing protocols
This protocol learns about the network by exchanging information with all the other nodes. By flooding the network with the beacons provide route table information of the network topology to be created. This method provides a quick way to update the route information by exchanging information with other nodes and get route information by referring to its table. But this method can be costly if the network is small and activity is minimal. However energy requirements are very expensive due to frequent transmission for maintaining of fresh topological data. Further space requirements are also taken into consideration if the node is also work as a router. Here some of the analysis of proactive routing protocols and its suitability with the proposed architecture are discuss below.

3.1 Dynamic destination sequenced distance vector routing protocol (DSDV).
DSDV is based on the bellman ford routing algorithm. Each node in the network maintains the entire destination and the number of hops. The updates are sent to each node either a full or incremental if there is a significant or periodic change in...
the network topology. In case of full dump a node transmits its entire routing table but an incremental dump only transmits the routing data that has changed. Full dumps are preferable when there is little movement in the network and updates are infrequent. Incremental ones operate more efficiently when the network is stable and network traffic is less consequential. Proposed architecture is more suitable for unstable network because if the nodes are compromised they try to send the wrong routing table update or frequently send the incremental update to confuse the neighboring nodes. Here neighboring IDS play a significant role to identifying the intruder or compromised nodes by exchanging the correct routing information or continuously checking the routing table with the routing information received from the neighboring nodes.

3.2 wireless routing protocol (WRP).

It is based on a shortest path algorithm. Each node maintains four types of information like a distance table, routing table, link cost table and a message retransmission list (MRL). Distance table maintains the distance data for each node (like node A maintains its neighbor B and C and B’s predecessor node). Routing table is a vector with the information for each known destination. Similarly link cost table has the information about the cost of routing information through each of its neighbors and the number of update periods received from each. An update message is periodically sent to each neighboring node. If the link is alive then the neighboring node should be response back by simple HELO message (if no route table changes) or an update routing table. If an updated routing table is received then the node uses this updated information to calculate better path. In this case if the node is worked as a cluster head then it can generate many attacks in the network but if the above proposed architecture is properly maintain in the each node then secure communication module of this architecture can protect many attacks.

3.3. Cluster Gateway Switch Routing Protocol (CGSR).

In this protocol the network is partitioned into cluster. Cluster head algorithm is used to combine the nodes into separate group. Election of a cluster head is done through separate algorithm. When a packet is sent it should be passes though the cluster head or simply send to the cluster head. It is then forwarded to another cluster head until it reaches the one that the destination node is a member. Suitability of the proposed architecture for the cluster head has been already discussed in the previous paper.

3.4. Global State Routing (GAR).

GSR is simply like link state routing and it improves upon DSDV by not flooding the network. Each node exchanges the vectors of the link states when it wishes to exchanges the routing table information. There are four information has been maintained for each node: neighbor list, a topology table, a next hop table and a distance table. Neighbor list contains the set of all the node’s neighbors. Topology table contains an entry for every destination. The next hop table maintains the information about the next hop to forward the packets. Distance table contains the information about the shortest distance between the two nodes. From the above specified table information each node is able to determine the network topology and routing decisions. Proposed architecture is working very efficiently because it has the complete information about the network topology and routing decisions.

3.5. Fisheye State Routing (FSR).

In FSR every update message does not contain information about all nodes in the network. Instead, information about the closer nodes is exchanged more frequently as compare to further nodes thus reducing the update message size. The center of the nodes has the most up to date information about all nodes in the inner circle and the accuracy of information decreases as the distance from the node increases. Proposed architecture is well suited in the central node as because the procedure of dividing the network into different scope levels is done at each node, meaning that it is Even if a node does not have the accurate information about the far away nodes, the packets will be routed correctly because the route information becomes more and more accurate as the packets gets closer to the destination. This means FSR scales well to large networks as the overhead is controlled [7, 11].

4. Reactive Routing Protocols

Reactive routing protocols are based on an on demand basis. Every node in this protocol maintains information regarding only active paths to the destination nodes. Since there is no need of periodic transmission of routing updates, reactive routing protocols are less resource intensive as compared to proactive routing protocols as because a route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Some of the examples of reactive routing protocols are as follows

4.1. Associativity-Based Routing (ABR).
This protocol selects the route based on the degree of association stability between the nodes. Each node periodically send the information regarding alerting its existence. Its neighbor updates its table by incrementing a tick value and greater the tick value the node is more static. When the information is no longer received, the tick value is reset. ABR protocol have three routing information: route discovery, route reconstruction and route deletion. Route discovery is initiates when a node wants to transmit a packet to a certain destination by sends out a broadcast query and waits for a reply. All neighboring nodes that receive the query replies back with their own address, associativity ticks with their neighbors and QOS information. Once the originating node receives all the reply then the route with the minimum number of hops is chosen to communicate with the destination node. Route reconstruction is needed when the route becomes unavailable due to link failure. Route notification is sent to all the downstream nodes to delete the respective entry information when an upstream node moves in the network. In the above proposed architecture is works more efficiently as because it expects high degree of association stability between the nodes. Further to detect and protect the intruder in the network route notification information is highly needed.


It is an on-demand route discovery protocol that uses two most important information regarding signal strength and location stability. Depending upo the strength of signals, SSA monitors weak and strong network channels. SSA uses two basic protocols SRP (static routing protocol) and DRP (dynamic routing protocol). DRP maintains signal stability table which stores the signal strength (strong/weak) of neighboring nodes that were discovered by way of information exchanges and a routing table. After processing this information, DRP passes it to SRP where the packet is then passed to the upper stack layer if it is the destination node. If not then the routing table is searched for a forwarding node. If no entry is found then a route request is performed using the strong channels for neighboring nodes. When the destination node receives the route request information it replies to the first packet. The DRP reverses the route, by sending the reply back to the requesting node. In case a link fails then the intermediate nodes return an error message to the requesting node. Then the source node informing all the nodes by sending an erase message that the link is broken and they can update this information accordingly. This proposed architecture demands continuous monitoring of the signal strength and location stability. Further information regarding link failure and stability is high acceptable to authenticate valid node in the network [15, 18].

### 4.3. Dynamic Source Routing (DSR).

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table update messages like table driven routing protocols do. For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (on demand routing). When a node wants to transmit a packet to a source destination, it consults the route cache. If the destination information is not known it initiates a route request. All the intermediate nodes checks the route cache for the availability of information on the destination node until it reaches a node that has information on the destination or reaches the destination node itself. On reaching the destination it generates a route reply message on information it has to reaching the destination. Proposed architecture is well suited for the DSR as because it does not consumed bandwidth by unnecessary sending huge information and the route cache is updated upon discovery of a new route for an entry.


CBPR divides the nodes in to clusters and also find a cluster head for nodes in a particular group using a cluster based algorithm. This cluster head is responsible for forwarding packet from one cluster head to another until it reaches the destination node. This similar process and suitability of the proposed architecture which is already discussed above with the proactive routing protocol cluster based routing. Its difference is that it uses an on demand and dynamic approach which is highly demandable in Adhoc network environment.

### 4.5. Ad Hoc On-Demand Distance Vector Routing (AODV).

AODV is a better version of DSDV. Broadcasts are minimized based on the demand for route information. One feature of AODV is the use of a destination sequence number for each routing table entry. The sequence number is created by the destination node. The sequence number included in a route request or route reply is set to requesting nodes. Sequence numbers are very important because they ensures loop freedom and is simple to program. Sequence numbers are used by other nodes to determine the freshness of routing information. If a node has the choice between two routes to a destination, a node is required to select the one with the greatest sequence number. AODV deals with routing table. Every node has a routing table. When a node knows a route to the destination, it sends a route reply to the source node. Route request (RREQ), Route Replies (RREPs) and Route Errors (RERRs) are message types defined by AODV. Proposed architecture is well suited for the AODV as because it provides loop free routing, optional multicast and also reduced control overhead. Further if the
source node moves it can reissue the broadcast request. In the event of a link failure, a special notification is sent to the upstream neighboring nodes which are very important to track the nodes and its location also to provide security measures.

5. Routing protocol security
Performing communication in free space exposes ad hoc networks to attacks as anyone can join in the network, and eavesdrop or inject messages. Ad hoc networks attacks can be classified as passive or active. Passive attack signifies that the attacker does not send any message, but just listen to the channel. A passive attack does not disrupt the operation of a protocol, but only attempts to discover valuable information. During an active attack, on the other hand, information is inserted into the network. The intrusion field studies how to discover that an intruder is attempting to penetrate the network to perform an attack. Most of the intrusion detection techniques are developed on a fixed wired network is not applicable in this new environment. In ad hoc network there are no traffic concentration points (switches, routers etc.) where the intrusion detection systems (IDS) can collect audit data for the entire network. The only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithm must rely on the partial and localized information. The proposed new intrusion detection architecture is distributed and cooperative in nature. Here all the nodes in the ad hoc network participate in finding intrusion detection and reaction. Each node is responsible for detecting signs of intrusion locally and independently, but neighbors can collaboratively investigate in a broader range. Besides that there are a number of security metrics that can be applied to limit these risks.

5.1. Encryption
Before the data is to be transmitted it must be encrypted by the node that is transmitting the data. Once the data is reached to the destination it must be decrypted by the node. There are number of encryption schemes that are already well known such as WEP and WPA. WEP is least used because its encryption is more easily broken. RSA and Diffie –Hellman algorithms are providing better security. However the encryption algorithm may be used is limited by the nodes in the network because of low energy, memory and computing power limit the complexity of the algorithm that may be used to provide better encryption [8, 10].

5.2. Authentication-Encryption. In this case the transmitting node includes its identification number and that same number is encrypted in the data header. When the receiving node receives the encrypted data it verifies the sender’s node identification and decrypts the encrypted identification number. If both identification numbers match, the data is forwarded. This measure basically prevents an intercepting node from imitating a legitimate node in the network. Although there are a number of various methods and techniques that can be used to securing the data between various nodes but to basic issues related to routing data between different nodes are
- Securing data in the event of interception and
- Preventing unauthorized data flooded in the network

5.3 secure routing protocols
Secure routing protocols basically provides additional security solution and measures to ad hoc networks.
5.3.1. Authenticated Routing for Ad Hoc Networks (ARAN). ARAN protect against third party attacks by using authentication, non-repudiation and message integrity. This is an on demand protocol that uses more secure method like digital signatures. Node uses route discovery packet when it wants communicates with other node. The IP field specifies the IP address of the destination node. Suppose node X wants to communicate with node Y in that case the message includes X’s certificate, a number that increases every time X sends a route discovery packet (RDP) and a time stamp. The message must be signed with the X’s private key. When the intermediate node like W receives the message, it verifies the authenticity by extracting X’s public key from the certificate within the message. After confirming that the certificate has not been expired, node W sets up a reverse route towards node X of the route discovery protocol. In case this is the first time node w has seen this message, it attaches its own certificate, signs the message with its own private key and rebroadcasts the route discovery protocol. Once the destination node Y receives the message , it authenticate the message by signing the message with its private key, IP address and certificate and sends a route reply( RREP) message. Nodes unicast the Route reply message to X through the discovered path. When route reply traverses the path, the intermediate nodes remove the certificate and signature of the previous node. But when route reply message reaches in the node X then it verifies the authenticity of the response.

5.3.2. ADRIADNE
This is an on demand secure ad hoc routing protocol based on DSR. It protects the compromised node in the network by using the symmetric cryptography. The target node provides the guaranteed authenticity of the originator by route reply. Adriadne provides authentication of a message routing using a message authentication code (MAC) and a shared key between two parties. For route reply request it uses time efficient stream loss tolerant authentication broadcast protocol to protect attacks from malicious nodes that attempting to modify the routing information, impersonation and wormhole attacks. But it does not provide protection against selfish nodes [3, 9].

5.3.3. Secure Ad Hoc On-Demand Distance Vector (SAODV).
It provides the source authentication, import authorization, integrity and data authentication services. It assumes the there is a key management system (KMS) that assigns keys to the nodes, verifying the association of the public keys and the node identities. A hash chain used to provides integrity for the hop count by applying a one way hash function to a random seed value. The source sets the hash value \( h \) to a seed \( s \) when transmitting the RREQ or RREP. When a node receives the message after \( n \) hops, it verifies the hash value with respect to time to live (ttl) value which is initialized by maximum hop count value. Every intermediate node applies a hash function to the message before forwarding to the current hash value. So that the top hash value \( T \) should always be derived. Once validated, the intermediate node i compute a new hash value by applying the hash function and forward it to the other nodes. This way source node signs everything but the hop count and the hash field which itself provide a better security [4, 8, 6].

5.3.4. Secure efficient Ad Hoc Distance vector (SEAD) Routing.
It provides secure distance vector routing with the limited resources of the nodes like network bandwidth, processing capabilities, memory and battery power. It provides better security in spite of active attackers or compromised nodes in the network. It uses one way hash function and too some based on destination sequenced distance vector routing protocol [12, 14].

5.3.5. Optimized Link State Routing (OLSR).
It is an optimized link state routing algorithm using multipoint relays (MPRs) that is selected nodes forward broadcast messages during flooding.
SECURITY ISSUES AND ITS CHALLENGES FOR HOST BASED MOBILE AD HOC NETWORKS TO PROTECT INTRUSION

Figure 3: Generic OLSR packet
The link state is generated by the MRPs. But the further optimization is done by the number of control messages [9, 11].

Figure 4: Flooding a packet in a wireless multi-hop network. The arrow shows all transmissions.
The MRP node may choose to report link states and MRP selectors: thereby providing only partial link state information in the network. From this information no of hop count is then easily calculated [3, 6]. OLSR is an optimization of a pure link state protocol for mobile ad hoc networks. First it reduces the size of control packets instead of all links; it declares only a subset of links with its neighbors who are its multipoint relay selectors. Secondly, it minimizes flooding of this control traffic by using only the selected nodes, called multipoint relays to diffuse its messages in the network. Only the multipoint relays of a node retransmit its broadcast messages. This technique reduces the number of retransmission in a flooding or broadcast procedure [5, 11, 12].
5.3.6 Malicious Nodes:
Malicious nodes affect the proper functioning of a wireless network routing protocol by modification of routing information and impersonating other nodes. They are used to redirect network traffic, deny service to legitimate nodes and compromise routing information by intentionally imitate authentic nodes, modifying the data content when transmitting the packet[2,8].

5.3.7 Selfish nodes:
Selfish nodes decrease the network performance by not participating in routing operation. This is not only to create an attack but also to conserve the energy of a node by not participating in network operation.

6. Criteria for Protecting Ad Hoc Networks

6.1 physical securities:
The significance of the physical security in respect to the overall protection of the network is highly dependent on the ad hoc networking environment in which the nodes operate. For emergency critical environment where the ad hoc networks
that consists of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security.

6.2 Security of Network Operations

Security of ad hoc networks can be based on protection in the link or network layer. However in most of the cases the security services are implemented in higher layers, for instance in network layer where routing plays a major role. To provide better security of network operation routing protocol must be protected from any attack against confidentiality, authenticity, integrity, non repudiation and availability [4, 5].

6.3 Better Service aspect:

Ad hoc network may consist of either hierarchical or flat infrastructure both in logical and physical layers independently. In such networks the necessary services like routing of packets and key management services have to distribute in such a way that all nodes have responsibility in providing the service. Availability is a central issue in ad hoc networks that must operate in dynamic and unpredictable manner. Since a node may be idle or shutdown once for a while or may be out of range due to movement of a node. Thus ad hoc network cannot make any assumptions about availability of specific nodes at any given time. For different commercial applications using ad hoc networks availability is often the most important issue from the viewpoint of the clients. In this networks where the area of application is highly dependent on the possible size of the network then assumption can be made about the scalability requirements of the security services as well.

6.4 Key Management security:

If public key cryptography is applied then the whole protection system is totally dependent on the security of the private key. If the physical securities of the nodes are not good enough then private keys have to be stored in the nodes confidentially, for instance encrypted with a system key. Further centralized approaches are also vulnerable as in the case of failure of a single node. So the mechanical replication of the private key or other information is an inadequate protection approach due its maintenance and the possibility of a node to be compromised. Then distributed and cooperative approach towards key management for any cryptosystems in use is needed.

6.5 Access Control and authorization

Access control is highly correlated to the authorization and identification as because the parties can be confirmed and authorize to gain access to the confidential information. Moreover the required security level in access control is dependent on the way the access control mechanism is implemented and affected in the network. But in case of centralized approach with low security mechanism is implemented as in the classroom or in seminar area then the access control can be managed by the server party with simple means of user id and password scheme. But without centralized approach with big scale ad hoc network then implementation of access control is much more difficult. The access to the network, its groups and resources must be defined in a proper manner when the network is formed and is very difficult. But if very complex, scalable and dynamic access control protocol is implemented which brings some flexibility to the user side but can generate many unknown attacks and it may even be impossible to apply properly and efficiently.

7. Conclusion

if security is the major concern in adhoc network then it is dependent on access control, proper authentication mechanism, communication between nodes and routing of packets and movement of nodes in the network also. In the above various routing protocols has been explored and its suitability with proposed architecture has been discussed. The security of a wireless system should never be reactive but proactive, anticipating vigorous and constant breach of attempts. More and more new attacks is generated the strengths of the security system is challenged. As the security requirements and their implications vary, provision for a general security architecture for ad hoc network cannot be constructed. The development of secure ad hoc networking framework seems to be just starting, as all the most severe security problems are not even fully solved in ad hoc networking area. There are still many challenges and research openings in the area of ad hoc networks security.

8. Future plan

In future some of the better authentication scheme has been implemented for proposed architecture to provide better authentication schemes and need to be combined with other security schemes like reputation and trust based schemes.

References


