Review of Various Attacks and a New Secure Data Transmission Mechanism for MANET

Ira Nath
JIS College of Engineering
Kalyani, Nadia

Prosenjit Chakraborty
JIS College of Engineering
Kalyani, Nadia

ABSTRACT

For transmission of data over Ad-hoc network, various routing protocols along with some lack of security are present. So, some attacks of different types may occur on data. As a result some important data may be captured by a stranger node. Here, a new algorithm has been proposed, through which accessing important data can be restricted by un-authorized user(s). This approach is to design a system that works with low cost & high security. So, using only one algorithm users can receive & send data surely with minimal cost by avoiding all possible attacks.

Keywords

MANET, Attacks, Security.

1. INTRODUCTION

[4,5,6] "Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station. For example, if it is needed to transfer a file to some one's friend's laptop, an ad hoc network may be created between the computer and the laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If it is needed to share files with more than one computer, a multi-hop ad hoc network could be set up, which can transfer data over multiple nodes. Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN). A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. MANET is vulnerable to different types of attacks. In this paper a description of different types of attacks are illustrated in section 2. Conclusion is depicted in section 4.

2. DIFFERENT TYPES OF ATTACKS ON MOBILE AD-HOC NETWORK

2.1 Black hole Attack [1, 2, 5]

A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. In a black hole attack, where attacker A (say) sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A. Several solutions exist to counter these types of attacks, among which it can be named as the technical estimate relation. In this mechanism the authors classified the relation between the nodes and their neighbors in three cases: Unknown (node X sent forever (received) of messages to (from) the node y and the probability of the malevolent behavior are very high), acquaintance (node X sent\ (received) some messages to (from) the node y and the probability of the malevolent behavior must be observed) and Friend (node X sent (received) in abundance of the messages to (from) the node y and the probability of the malevolent behavior is too small. This mechanism is implemented in the routing protocol RDSR (Relationship enhanced DSR protocol) [3]. The Threshold of sequence number consists in performing a check to find if RREP sequence no is higher than the threshold value. The threshold value is dynamically updated in each time interval. As the value of RREP sequence no proves higher than the threshold value, one suspects the node to be malicious and adds it to the black list. This mechanism is implemented in the routing protocol DPRAODV (Detection, Prevention and Reactive AODV). The Watchdog or monitoring (watchdog) is a solution which makes it possible to identify malicious nodes. The Watchdog assigns positive values with a node which successfully forwarded packages and a negative value after a threshold level of bad behavior was observed. It's implemented in SWAN (mobile Secure Watchdog for Ad hoc Network). Path rater which makes it possible the protocol to avoid nodes corrupted register in a black list [9]. The DRI or the data table of information's routing which is used to identify nodes of cooperative black hole, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for" TRUE " for intermediate nodes answering the RREQ of node source, AODV implements this mechanism .

2.2 Wormhole Attack [2,3, 4]

Wormhole Attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality [1][2]. To fend off the Wormhole attacks some authors proposed to use the concept of Hop-count Analysis. In this mechanism, a route which has a low or high hop counted is considered to be non usable. A so low hop counted can imply an attack of wormhole; while a high hop can also slow down the transmission. The protocol Multipath Hop-count Analysis (MHA) implements this mechanism and also protocol AODVWADR (AODV) Wormhole Attack Detection Reaction. The clustering consists in dividing the network clusters with for each one a head and members. When a node in the cluster suspects an attack wormhole of the layer1 in the cluster, it informs the head of the item cluster. The heads of the clusters of the layer1 inform its members respectively. This mechanism is implemented in the protocol in AOD. The protocols LAR (Location Aided Routing) et AODVWADR (AODV Wormhole Attack Detection Reaction) implement this mechanism [1] and also the directional antennas (Directional antenna) which consists in using the direction of the packets of arrival to detect if the packets come from their own neighbors. This solution is implemented in DREAM (Distance Routing Effect Algorithm for Mobility).

2.3 The Selfish Attack[1]

The Selfish Attack consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit. To prevent the selfish nodes some solutions were proposed. Among these, one method has a solution based on the Negative Selection Algorithm (NSA). It’s based on the principles of the discrimination of self or no self in the immune system (to define it to oneself like a collection S of elements in a characteristic space X, a collection which needs to be supervised). The detection of anomaly aims at distinguishing a new model like part of self or no-self, given a model of system of self. Structured GA (SGA) is a type of evolutionary algorithm which incorporates the redundant genetic material, which is controlled by a mechanism of gene activation. It uses the multi-layer genomic structures for its chromosome i.e. all the genetic material (expressed or not) is structured in a hierarchical chromosome. The activation and deactivates mechanism these coded genes. This solution is implemented in AODV. A solution based on the reputation (CORE and CONFIDANT) which consists in collecting information on an old behavior of the tested entity by others. A solution based on the payment (Neglect) which requires with nodes which benefit from the resources of the network (transmitters and/or receivers) to pay “service providers” (intermediate nodes) and a solution based on the localization (directional antennas).

2.4 Routing Tables Overflow [1,2,3]

Routing Tables Overflow consists of malicious nodes to cause the overflow routing tables of nodes being used as relay. To fend off this attack the named solution Trust evaluation was proposed. It’s based on the evaluation of confidence to ensure a secure routing in MANETs. The success of a communication through a node will increase the index of confidence of this node and the failure by this node will decrease the index of confidence. If this value reaches zero this node is registered in a blacklist and we inform the other neighbors. TRP (Trust-based Routing Protocol) implements this solution.

2.5 Flooding Attack[2,3]

Flooding Attack makes it possible for an adversary to carry out DoS by saturating the support with a quantity of broadcasting messages, by reducing the output of nodes, and in the worst case, to prevent them from communicating. To prevent saturation on the level of nodes two principal approaches were proposed. An approach based on the Relationship, in this mechanism, all the nodes in an ad hoc network are classified by categories: friends, knowledge or foreigners, based on their relationship with their neighbor nodes. During the initialization of the network all the nodes will be foreigners between them. A confidence estimator is used in each node to evaluate the degree of confidence of his neighbors. This solution is implemented in protocol AODV). An approach based on the virtual currency which uses the concept of credit or micro payment to compensate for the node service. An approach based on the method of neighbor suppression (FAP). When the attacker diffuses a large number of RREQ packets, the neighbor nodes to the attacker record the rate of requests for routes. Once the threshold is exceeded, the neighbor nodes deny all the future packets of request of the attacker. There are many attacks and the protocols which implement these above mentioned mechanisms do not resist with these types of attacks. The following table recapitulates the protocols and the attacks which the protocols can counter.

2.6 Packet misrouting attacks [1,2,3]

In packet misrouting, a malicious node relays the packet to the wrong next-hop, which results in a packet drop. Note that, in basic LM, a node that receives a packet to relay without being in the route to the destination either drops the packet or sends a one-hop broadcast that it has no route to the destination. The authors in argue that the latter case would be more expensive and dangerous since it gives malicious nodes valid excuses to drop packets. Therefore, they go with the first choice, even though it may result in some false accusations. In this attack, a malicious intermediate node achieves the same objective as if it were dropping a packet. However, none of the guard nodes using basic LM become any wiser due to the action. In addition, some legitimate node is accused of packet dropping.

2.7 Impersonation attacks [2,3,4]

The impersonation attacks, also called the spoofing attacks, are attacks where malicious node assumes the identity of another node in the networks. By impersonating another node, attackers are able to receive routing messages that are directed to the nodes they faked. Impersonation attacks are possible in the ad hoc networks because most of the current ad hoc routing protocols do not authenticate the routing packets. As a result, malicious nodes might exploit this loophole to masquerade as another node by modifying the contents of the packets.

2.8 Routing packet analysis attacks [1,3,6]

Since no disruptive action occurs, routing packet analysis could be classified as one of the passive attacks against the ad hoc networks. One way to launch this attack is by exploiting the promiscuous mode employed in the ad hoc network. In a promiscuous mode, if node A is the neighbor of both nodes B and C at a particular time, node A can always hear the transmissions between node B and node C. By exploiting this nature, node A is able to analyze the overheard packets transmitted between node B and node C. More explanation regarding the promiscuous mode in the ad hoc networks can be found. Besides, malicious nodes could also launch this attack by exploiting the nature in a multi hop routing. In multi hop routing, packets need to be forwarded through several intermediate nodes before reaching the actual destination. Malicious nodes might exploit this opportunity by locating themselves in any location along the route to participate in the message forwarding process and later launch the routing packet analysis attacks.

2.9 Packet dropping attacks [1,2,5]

Direct interruption to the routing messages could be done by using the packet dropping attacks. In a standard packet dropping attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behavior remain concealed.

2.10 Sleep deprivation attacks [1,2,6]

This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks.

2.11 Route salvaging attacks [1,3]

Route salvaging attacks are launched by the greedy internal nodes in the networks. In a mobile ad hoc network, there is no guarantee that each transmitted packet will successfully reach the desired destination node. Packets might not reach the destination node because of the natural network failures or might be under attacks by the adversaries. Therefore, to salvage their packets from such failures, misbehaving internal nodes might duplicate and retransmit their packets although no sending error messages received. The effects of the route salvaging attacks might be more severe if there are many greedy nodes in the networks. Besides draining off more resources in intermediate and destination nodes, this attack might also cause the consumption of unnecessary bandwidth.

2.12 Lack of cooperation attacks [2,3,4]

Lack of cooperation from the internal nodes to participate in the network operations can also be seen as an attempt to launch a refusal of service attack. In such attacks, internal nodes are discouraged to cooperate in the network operations that did not benefit them because participating in such operations will drain off their resources. Misbehaving internal nodes might use different strategies to save their limited resources. They might refuse to forward the other node's packets, not send back the route error report to the sender when failing to forward packets, or might turn off their devices when not sending any packet in the networks.

2.13 Modifying route metrics [1,2,3]

The process of reverse path setup in reactive route discovery means that nodes have to rely on routing metric information, contained within a control packet, to determine the best route to the packet's originator. The routing metrics used by reactive protocols are typically cumulative distance vector metrics, such as the number of hops. If a malicious node receives a route request or reply, then it could falsely decrease the hop count metric before forwarding the packet. However, even if the malicious node advertises a falsely low metric of zero hops, the number of hops in the control packet will increase as it propagates away from the malicious node.

2.14 Rushing attacks [2,3]

The nature of reactive route discovery means that reactive routing protocols are much more sensitive to network conditions than proactive routing protocols. This sensitivity can be exploited by malicious nodes. For example, a malicious node could rebroadcast route requests quicker than its neighbors'. This is also known as a rushing attack. One method to achieve this is to exploit the Medium Access Control protocol, which will typically delay broadcasting of packets to avoid broadcast storms. A malicious node could ignore the delay, broadcast the request before its neighbors can, and, hence, increase the likelihood of being part of the final established route. Another method of realizing a rushing attack is to use a wormhole, discussed in more detail below.

2.15 False route replies[1,3]

In order to improve the scalability of routing, reactive routing protocols typically trust intermediate nodes to reply to requests when they have an up-to-date route to the requested destination. Therefore, another way for a malicious node to coerce the network to send packets to it is to reply to route requests regardless of whether it has a route or not. Using attractive metrics will increase the probability of success.

2.16 False gratuitous route replies[2,3]

AODV has a mechanism to ensure that only bidirectional routes are discovered; intermediate nodes which issue a reply also have to inform the requested destination by uni-casting a gratuitous reply to it. Thus, the destination node and the intermediate nodes which receive the gratuitous route reply will all add or update a route to the request originator. A malicious node could target nodes and send them gratuitous replies, claiming that they have been subject to route discovery. If the malicious node uses attractive metrics, then those nodes will update their routing tables to route through the malicious node.

2.17 False removal of working routes [1,3]

Most reactive routing protocols rely on a route maintenance mechanism to prevent nodes from sending packets for routes which are no longer active. If unprotected, the route maintenance mechanism is highly vulnerable to attack. If the malicious node is part of the route, then it could send route error messages to force all upstream nodes to mark the route as inactive. Even if a malicious node is not part of a route, but is nearby, then it may masquerade as an intermediate node and send a spoofed route error message. Alternatively, a malicious node could store a route error packet, perhaps induced earlier as a result of a denial of service attack, and replay it at a later time; typically, route error messages do not include a means of checking for freshness. One effect of such an attack is that nodes will falsely believe the route is broken, and may waste resources in trying to discover another route, which could in fact be the same route that was used before the attack. Proactive routing protocols do not have an explicit link recover mechanism. Instead, link breaks are inferred when a node stops advertising a link to a neighbor. Unless the protocol makes use of triggered updates, there will be a delayed reaction until the next periodic update packets are flooded. Thus, proactive protocols are more robust against such an attack, as there is no means of falsely inducing route breaks. Instead, the malicious node has to rely on other denial of service attacks, such as impersonating a node on the route in order to spoof Hello messages containing empty sets of links.

3. PROPOSED WORK

3.1 Assumption

- Each node has same transmission range.
- All the connections are found at **tth** time. At (t+1)th time , some new node may be added into to this network & some existing node may be disconnected.
- Initially maximum cost is fixed. If least no. of paths found them may change.

3.2 Word abbreviation

1. MTU - Maximum Transfer Unit
2. ACK - Acknowledgement

3.3 Algorithm

3.3.1 Algorithm 1

Step 1: Start.

Step 2: Data stored into a text file by sender & check the size of that data.

Step 3: Broadcast a route request over the network (ad-hoc) to search destination position at tth time.

Step 4: Sender should receive one or more than one route reply from receiver. So, sender should get all possible paths.

Step 5: Sender now checks, how many no. of paths are found. Go to *step 5*. If any path not found then go to *step 8*.

Step 6: Weather if found more than β paths then select max MTU of those paths & count no. of path which have selected MTU.

Step 7: If no. of path β is sufficient then data will be fragmented according to that MTU (mean size by size) & data will be sent through all the paths which have that MTU. Otherwise decrease the selected MTU & again check no. of paths. Until no. of path β is sufficient, this process will go on till selected MTU=1. Then go to step 9.

Step 8: If selected MTU= p then data should be divide by ‘p’ size each.

Step 9: If ‘n’ no. of paths is found & no. of data fragment is (2n+3), then all ‘n’ no. of paths carry data fragments one after another. After that there also (n+3) no. of fragment are ready to transmit.

Step 10: But sender first checks whether all the data which are previously sent are successfully received or not. Else retransmit those data first then new data should be transmitted.

Step 11: For each fragments receiver should check sender’s address from which it had received route request.

Step 12: After receive all fragments, receiver should be done concatenation operation.

Step 13: Receiver now gets whole data.

Step 14: Stop.

3.3.2Algorithm 2

Step 1: Start

Step 2: According to **algorithm 1** best routes selection, data fragment creation & sending of created data fragment can be done optimally.

Step 3: If primary destination’s address of each data fragment is matched with receiver’s address, then only data will be received.

Step 4: Stop.

3.4 Drawbacks

This algorithm is secured for several attacks but it has some drawbacks also.

- If IP spoofing occurs then it may not properly work.
- If first node of each path is same & if that is worm then data should be taken by an unauthorized user.
- Here we assume that all the nodes have same transmission range, but in real world transmission range may not be same.
- Here we assume all the connections is found at tth time. So at (t+1) th time all the connections may be changed. This is not considered here.

4. CONCLUSION

The aim of the paper is to study about the different types attacks in the ad-hoc network. Try to restrict those attacks those attacks & save the data & information. That’s why here a new security concept is designed which may protect data from several types of attacks. An overview of the existing security scenario in the ad-hoc network environment has been proposed. Ad-hoc routing & intrusion detection aspect of wireless ad-hoc networks were discussed. Ad-hoc networking is still a raw area of research as can be seen with the problems that exist in these networks & the emerging solutions. The key management protocols are still very expensive & not fail save. Several protocols for routing in ad-hoc networks have been proposed. There is a need to make them more secure & more robust to adapt the demanding requirements of these network. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment.

5. REFERENCES

[1] Ms. N.S.Raote* et al. “Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network”, INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES(IJAEST) Vol No. 2, Issue No. 2, 172 - 175

[2] YIH-CHUN HU, ADRIAN PERRIG, DAVID B. JOHNSON, “Ariadne: Secure On-Demand Routing in Ad-Hoc Networks”, Springer Science Business Media, Inc. Manufactured in The Netherlands, Wireless Networks 11, 21–38, 2005.

[3] Ahmad Alomari, Marius Iulian Mihailescu, “Improvement authentication of routing protocols for

Mobile Ad Hoc networks", 2012 International Conference on Industrial and Intelligent Information (ICIII 2012) IPCSIT vol.31, IACSIT Press, Singapore, 2012.

[4] http://techterms.com/definition/adhocnetwork.

[5] http://airccse.org/journal/ijdps/papers/1111ijdps28.pdf.

[6] https://en.wikipedia.org/wiki/Mobile_ad_hoc_network.