Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

SECURITY IN MANET: ATTACKS AND SOLUTIONS

V. Harsha Shastri[1], V.Sreeprada[2]

[1] Research Scholar, Dept. of CSE, Sun Rise University, Alwar, Rajasthan, India
[2] Lecturer, Dept. of Computer Science, St. Mary's Centenary Degree College, Secunderabad, TS, India

Abstract: *Security is a primary concern and the communication between the mobile nodes must be protected. The mobile ad hoc network (MANET) pose a number of challenges in the security design such as shared wireless medium, resource constraints, and highly dynamic network topology. A MANET is an infrastructure less network and an autonomous system of mobile nodes connected by wireless links. Each node operates not only as a host but as a router to forward the packets. The nodes are free to move and organize themselves into a network. They change positions frequently. Nodes can directly communicate to all other nodes within the radio communication range. If a node could not have direct communication then they can use intermediate nodes to communicate with other nodes. The security is of major concern and there are more chances for vulnerabilities. The attacker may use different approaches to decrease the network performance and throughput. In this paper, the principal focus is on the security criteria of the mobile ad-hoc network and presents the main attack types that exist in it. Finally we survey the current security solutions for MANET.*

***Keywords**: Mobile Ad hoc Network, Security, Attacks, solution, wireless network*

I. INTRODUCTION

A Mobile Ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. These nodes organize themselves and form a network dynamically. It is a collection of wireless network which consists of large number of mobile nodes. Nodes in MANET can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirement for secure networking is secure protocols which ensure confidentiality, integrity, availability, and authenticity of the network. There are many existing security solutions for wired network which are ineffective and inefficient for MANET. The transmission takes place in an open medium so MANET is vulnerable to many attacks. The nodes dynamically establish path in order to communicate with each other. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Ad-hoc networks do not rely on any pre-established infrastructure, so therefore they can be even deployed on places with no infrastructure. So it's useful in disaster recovery situations. Ad-hoc networks are helpful in conferences where people participating in conference can form a temporary network without engaging in services of any pre-existing network [2]. So the Mobile ad-hoc networks might be more prone to security issues as compared to wired networks.

Security is an important issue in the integrated MANET-Internet environment because in this environment the attacks on Internet connectivity and also on the ad hoc routing protocols are of main concern. Such dynamism of MANET-based architectures leads to some inherent weaknesses and a wide variety of attacks target these weaknesses. In this paper, we discuss some of the existing malicious attacks against MANETs and also the solutions to defend against them.

II. Security Goals

In MANET, the nodes are self organizing which act as a host as well as router. Securing a MANET is challenging task.
The goals to evaluate if a MANET is secure or not as follows:

- **Availability:** the assets are accessible to authorized parties at appropriate times. Availability applies to both the data and services. It ensures that the network service is survivable despite denial of service attack.
- **Confidentiality**: it ensures that the computer assets are accessed by authorized parties only. To maintain confidentiality of some confidential information, we need to keep them secret from all the entities that do not have privilege to them. It is some times called secrecy or privacy.

- **Integrity**: assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.
- **Authentication**: it enables that the node should ensure the identity of the peer node it is communicating with. Participants in communication are authenticated. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.
- **Non-repudiation**: the sender and receiver of the message cannot disavow that they have never sent or received the message. This is helpful when we need to discriminate if a node with some undesired function is compromised or not.
- **Anonymity**: all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.
- **Authorization**: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

III. Vulnerabilities in MANET

Vulnerability [1] can be described as a weakness in the security system. A system may be vulnerable to unauthorized data manipulation because the system does not verify user‟s identity. MANET is more vulnerable than wired network. The following are the vulnerabilities:

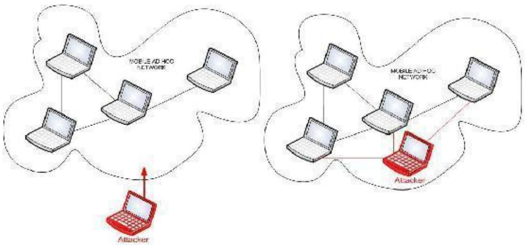
- **Lack of centralized management**: MANET does not have centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large-scale ad-hoc network.
- **Cooperativeness**: Routing algorithm for MANET assumes that the nodes are cooperative and non-malicious. As a result, a malicious attacker can become a routing agent and disrupt the network operation.
- **No predefined boundary**: We cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment as the nodes join and leave the network. As soon as the adversary comes in the radio range of a node it will be able to communicate with that node.
- **Adversary inside the network**: The mobile nodes within the MANET can freely join and leave the network. The nodes may also behave maliciously. This is hard to detect that the behaviour of the node is malicious.
- **Limited power supply**: The nodes in the MANET need to consider restricted power supply. The nodes may behave in a selfish manner where it is finding that there is only limited power supply.

IV. Attacks in MANET

Securing wireless ad-hoc networks is a highly challenging issue. Security of communication in MANET is important for secure transmission of information [Hass et al].Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

- **External attack**: It is carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

- **Internal attack**: These attacks are form compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyse traffic between other nodes and may participate in other network activities.



- *Figure 1: Internal and external attack*

- **Denial of service attack:** This attack aims to attack the availability of the node or entire network. If the attack is successful, then the services are not available. The attacker uses signal jamming and battery exhaustion method.
- **Impersonation**: If authentication is not properly implemented a malicious node can act as genuine node and monitor the network traffic. It can send fake routing packets, and gain access to confidential information.
- **Eavesdropping:** It is a passive attack. The node simply observes the confidential information and later this information is used by malicious node. The secret key information like public and private keys, location, password etc can be fetched by eavesdropper.

- **Routing attacks:** the malicious node makes the routing services as a target because this is important in MANET. There are two types of routing attack. One is an attack on the routing protocol and other is an attack on packet forwarding or delivery mechanism. In the first type of attack, the information regarding the routing to a node is blocked. In the next type, the packet delivery is disturbed against a predefined path.
- **Black hole attack:** In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it [4]. 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. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.
- **Worm hole attack**: an attacker receives packets at one point in the network, ―tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

V. Routing Protocols in MANET

Ad-Hoc routing protocols are commonly divided into three main classes; Proactive, reactive and Hybrid protocols. The figure 2 shows the routing protocols:

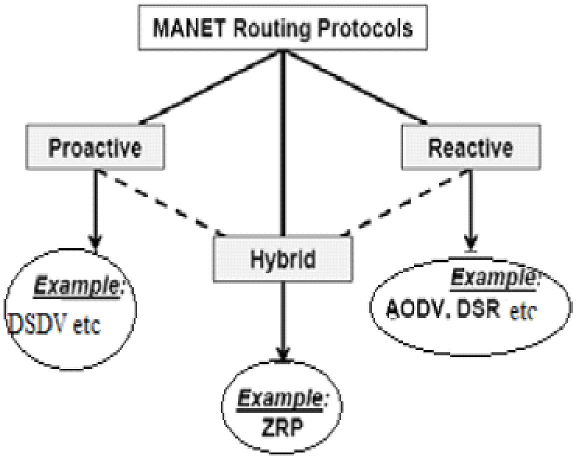


Figure 2 various routing protocols.

- **Proactive protocols**: It is also known as table driven protocols. They maintain the routing table of entire network constantly. Each node has to maintain one or more tables to store routing information and response to changes in network topology by broadcasting and propagating. The routing tables are updated constantly whenever the network topology changes in order to have a consistent view. Each node in the network sends a broadcast message to the entire network if there is any change in the network topology. This leads to maintenance of the routing table because the entries must be updated and must provide the actual information of the entire network. For a large network, proactive routing protocols are not recommended as it leads to overloading of the routing table and more bandwidth. consumption. Examples are DV (distance vector) , DSDV(Destination sequenced distance vector), OLSR (optimal link state routing) and WRP (wireless routing protocol).

- **Reactive protocols**: It is also known as on-demand routing protocols. They maintain or discover routes only on demand. A control message is flooded to the routes to discover the appropriate route. A route is established only when a node in the network wants to send a message to another node in the network. It has an advantage because the routing table is not overloaded but there is long delay in establishing the route. Examples are DSR (Dynamic source routing), AODV (Ad-hoc on demand distance vector routing), LAR (location aided routing) and TORA (temporally ordered routing algorithm).

- **Hybrid protocols**: It is a combination of reactive and proactive routing protocols. It is basically used to overcome the disadvantages of both routing protocols. It uses the route discovery and on demand mechanism of reactive routing protocol and the routing table management mechanism of proactive routing protocol. A large network is divided into zones. The routing within zones is done by using proactive approach and the routing outside the zone done by using reactive approach.

VI. Routing Attacks

Generally there are four different type of attack in MANET which are broadly classified into two main types:

- Routing disruption attack.
- Resource consumption attack.

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth.

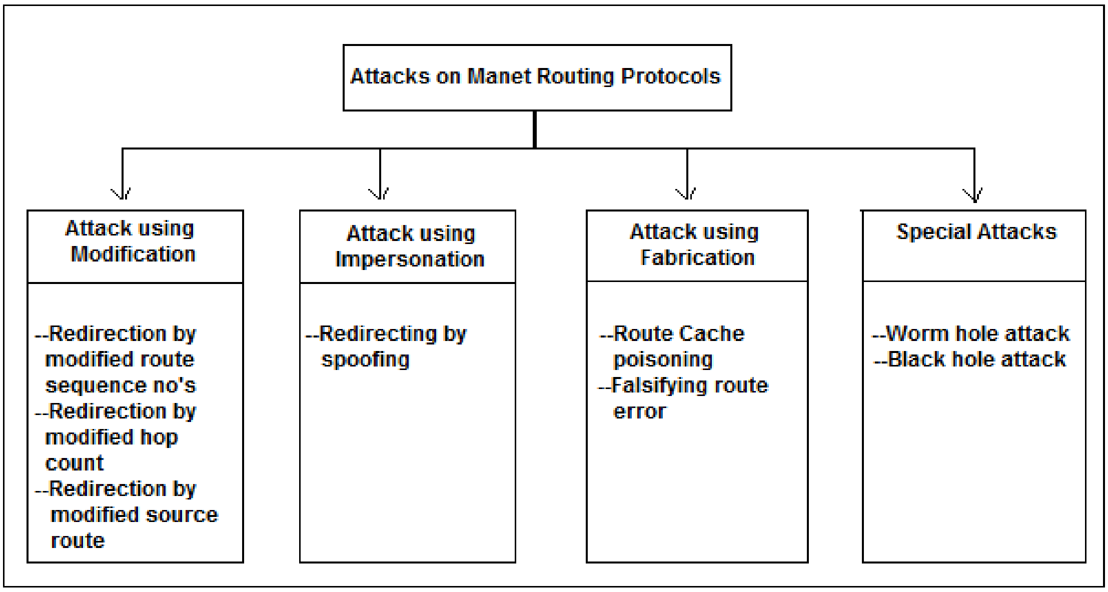

Attacks on Manet Routing Protocols
Attack using Modification
--Redirection by modified route sequence no's
--Redirection by modified hop count
--Redirection by modified source route
Attack using Impersonation
--Redirecting by spoofing
Attack using Fabrication
--Route Cache poisoning
--Falsifying route error
Special Attacks
--Worm hole attack
--Black hole attack

Figure 3 shows classification of attacks in MANET routing protocols [10] as:

Attacks using modification: Some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. Some of these types of attacks are given below:

a. **Route seqeunce numbers modification:** In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets**.**

b. Hop count modification attack : In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

c. **Source route modification attack :** In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Figure 4 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X) which shows that node S and the node X cannot communicate each other directly, and in the scenario where the node M which act as a malicious node which are going to attempt a denial-of-service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try to send the picket towards the destination X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

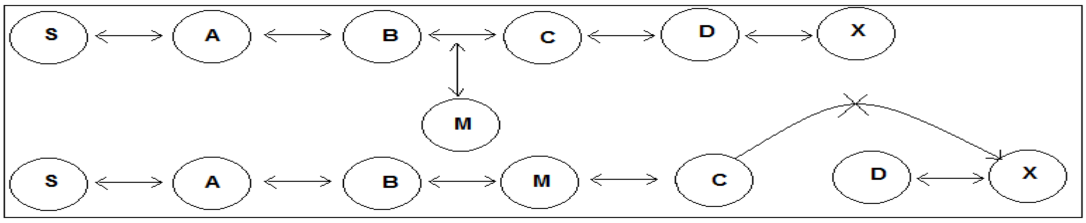


Figure 4 shows an example of route modification attack.

d. **Attacks using impersonation:** In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. The figure 5 shows this type of attack:

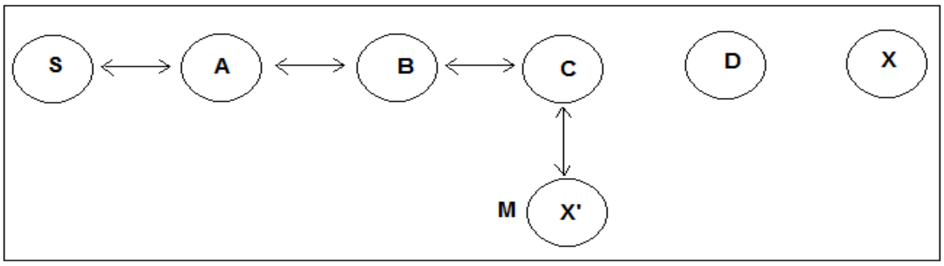


Figure 5 shows type of impersonation attack.

In the above figure where the S node wants to send data to the node X and for that it first starts Route Discovery process. During this process a malicious node M receives route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

e. **Attacks using Fabrication:** In this type of attack, an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. In Figure 6 where fabrication attacks is explained by an example. Here the source node S wants to send data towards the destination node X, so therefore at the beginning it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

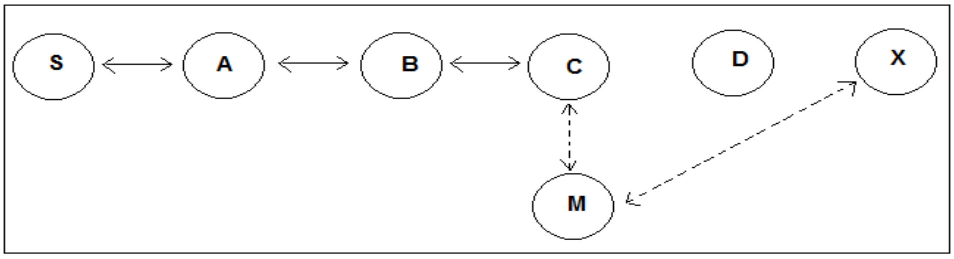


Figure 6 shows fabrication attack

f. Special attacks: There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

- **Wormhole Attack:** The wormhole attack [3] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 7 which is given below:

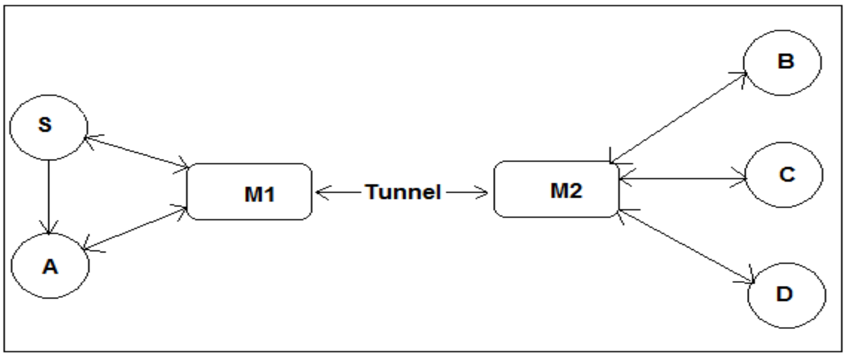


Figure 7: Worm hole attack Example.

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes [3], which are used to authenticate nodes among each other by timing information process.

- **Black hole attack:** In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other. Figure 8 shows the black hole attack.

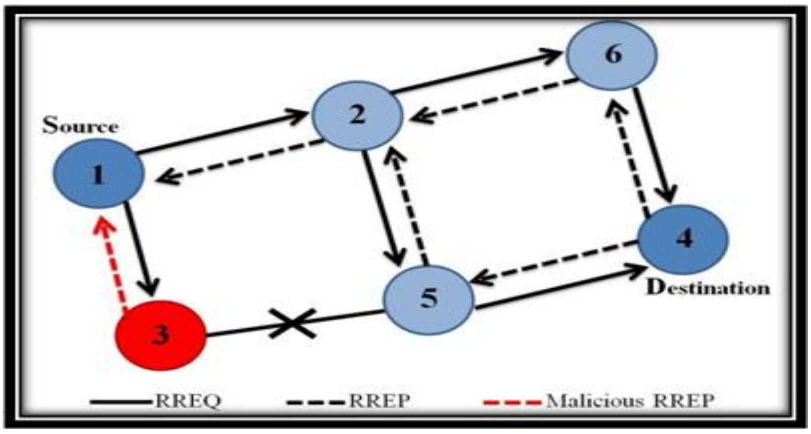


Figure 8: Black hole attack Example

VII. Security solutions to avoid attacks in MANET

Secure Multi casting: It is a mechanism where any user becomes the part of multicast group and even send traffic to multicast users as well as receive traffic, but as a result of this procedure it easily falls into the denial of service attacks. An architecture that is used to secure multicast traffic is DIPLOMA which stands for Distributed Policy enforcement architecture. It is used to protect or secure end services as well as network bandwidth. Audio and video usually falls into multicast traffic used by militaries as well as disaster back up teams. Responsibilities of DIPLOMA are:

- It gives solution for both sender and receiver whenever they access to the multicast group
- It also used to limit the bandwidth
- DIPLOMA integrates with common multi casting routing protocols like PIM-SM and ODMRP.
- It also uses to provide (allocate) network resources in a fair manner during attacks.

Secure Routing: MANET is vulnerable to attacks and can easily damage the whole network; it is be some of the mobile nodes are compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication

Responsibilities:

- It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
- Routing protocol responsiveness itself provide safety among different routing attacks.

Privacy- aware and Position based Routing: MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that's why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbors. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

Key Management: Certified Authority (CA) [2] is one of the mechanism which provide key management; if it is compromised then entire network can easily be damaged. One of the major functionality is it provides solutions for mobility related issues. The approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

Intrusion detection System: It is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behavior. IDS use to detect critical nodes and then analyze its data traffic, critical node also degrade network performance. There are different IDS systems which have some specific features like:

- Cluster based voting
- Neighbour monitoring
- Trust building

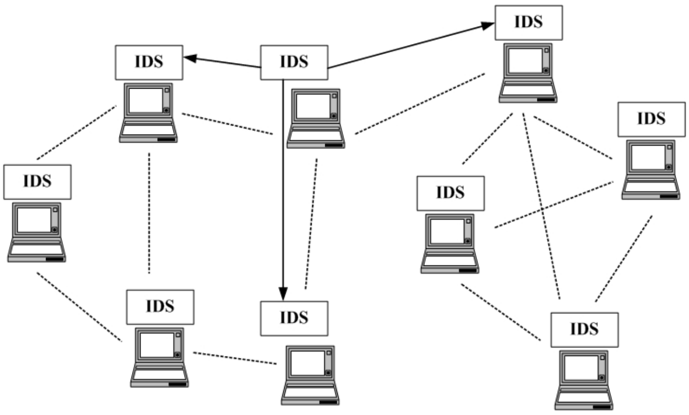


Figure 9: An IDS architecture for MANET

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder.

VIII. Measures to protect the MANET from black hole attack

Measures for black hole attack: Some secure routing protocols, such as the security-aware ad hoc routing protocol (SAR), can be used to defend against black hole attacks. The security-aware ad hoc routing protocol is based on on-demand protocols, such as AODV or DSR.

In SAR, a security metric is added into the RREQ packet, and a different route discovery procedure is used. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. At intermediate nodes, if the security metric or trust level is satisfied, the node will process the RREQ packet, and it will propagate to its neighbors using controlled flooding. Otherwise, the RREQ is dropped.

If an end-to-end path with the required security attributes can be found, the destination will generate a RREP packet with the specific security metric. If the destination node fails to find a route with the required security metric or trust level, it sends a notification to the sender and allows the sender to adjust the security level in order to find a route. To implement SAR, it is necessary to bind the identity of a user with an associated trust level. To prevent identity theft, stronger access control mechanisms such as authentication and authorization are required.

In SAR, a simple shared secret is used to generate a symmetric encryption/decryption key per trust level. Packets are encrypted using the key associated with the trust level; nodes belonging to different levels cannot read the RREQ or RREP packets. It is assumed that an outsider cannot obtain the key. In SAR, a malicious node that interrupts the flow of packets by altering the security metric to a higher or lower level cannot cause serious damage because the legitimate intermediate or destination node is supposed to drop the packet, and the attacker is not able to decrypt the packet. SAR provides a suite of cryptographic techniques, such as digital signature and encryption, which can be incorporated on a need-to-use basis to prevent modification.

IX. CONCLUSION

Mobile Ad-hoc networks (MANET) are prone to various kinds of vulnerable attacks since they are dynamic, wireless and infrastructure less network In this paper, we try to inspect the security issues in the MANET. Due to the mobility and open media MANET is prone to all kind of security risk such as intrusion, denial of service attack or information disclosure. The security needs in the MANET are much higher than those in traditional wired networks. Mobile Ad Hoc networks need very specialized security methods. There is no approach fitting all networks, because the nodes can be any devices. The computer security in the nodes depends on the type of node, and no assumptions on Security can be made.

REFERENCES

[1] Chang Li Shi, Lan Yang Hao, Sheng Zhu Qing (College of Computer Science Chongqing University Chongqing, China). Research on MANET Security Architecture design.

[2] Biswas, J.; Nandy, S.K.(2006),Efficient Key Management and Distribution for MANET, Communications. ICC '06. IEEE International Conference on , vol.5, no., pp.2256-2261,doi: 10.1109/ICC.2006.255106.

[3] Chlamtac, I., Conti, M., and Liu, J. J.-N.(2003), Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), pp. 13–6.

[4] Broch,J., A.M David and B. David(1998), A Performance comparison of multi-hop wireless ad hoc network routing protocols. Proc.IEEE/ACM MOBICOM'98, pp: 85-97.

[5] IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.

[6] Joshi Nikhil R, D.N Chandrappa,"MANET Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity"

[7] Sudip Das, "Security issues in Mobile Ad-Hoc networks"

[8] Kaman his Biswas, Mohd. Liakat Ali. "Security Threats in Mobile Ad-Hoc Networks".

[9] Yi-an Huang and Wenke Lee(September 2004) ,Attack analysis and Detection for Ad-hoc Routing protocol. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France

[10] Magnus Frodigh, Per Johansson and Peter Larsson. Wireless ad hoc networking— The art of networking without a network.