ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Study on Security Attacks And Key solutions for MANETs by Onion Routing

PRIYANKA M S[1], Asst.Prof. SRIVINAY[2]

Department of CSE, AIT, Bangalore, Karnataka, India[1,2]

Abstract: Wireless sensor network is a network which is having sensors used for communication. It plays a vital role in today's world. The major parts of WSN are Mobile Adhoc Network (MANETs). MANET is having mobile platforms and is freely moving. In MANET the connectivity nodes changes frequently. The MANET network thus needs to be authenticated, where authentication is a form of authorization which gives access to system based on identity.

Keywords: Mobile Adhoc Network (MANETs), On-demand routing protocols, security Mechanisms**,** Anonymous protocol for MANETs, security attacks.

I. INTRODUCTION

MANETs are formed by wireless hosts which may be mobile nodes, and there is no pre-existing infrastructure, so called as infrastructure less networks. Routes between nodes may potentially contain multiple hops. The Nodes acts as routers to forward packets for each other Node mobility may cause the routes change. Fig 1.1 shows that as the nodes changes its position in the network the route also changes. There are many advantages of the MANETs low-cost, flexibility Ease & Speed of deployment, decrease in dependence on infrastructure.

- Decreased dependence on infrastructure supply, a radio, and an actuator.1 A variety of mechanical,

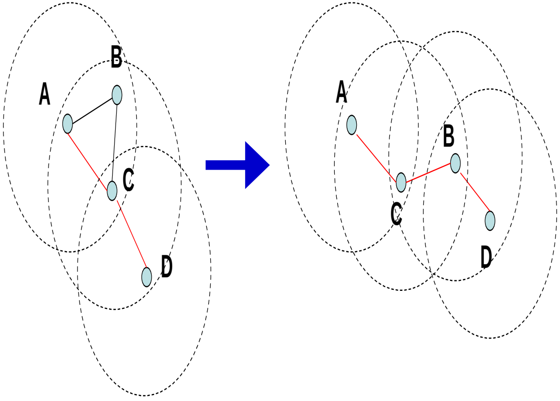


Fig 1.1: As node mobility changes route changes.

Deployment, decreased dependence infrastructure. The applications of MANETs are Military environment soldiers, tanks, planes Civilian environments vehicle networks conferences / stadiums outside activities Emergency operations search-and-rescue / policing and fire fighting.

DSR

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbours of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. The destination node, on receiving a Route Request packet, responds by sending a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received. This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated.

The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols.

Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length. Packet header size grows with route length due to source routing; Flood of route requests may potentially reach all nodes in the network. Potential collisions between route requests propagated by neighboring nodes. Increased contention if too many route replies come back due to nodes replying using their local cache Stale caches will lead to increased overhead.

DOI 10.17148/IJARCCE.2015.45110

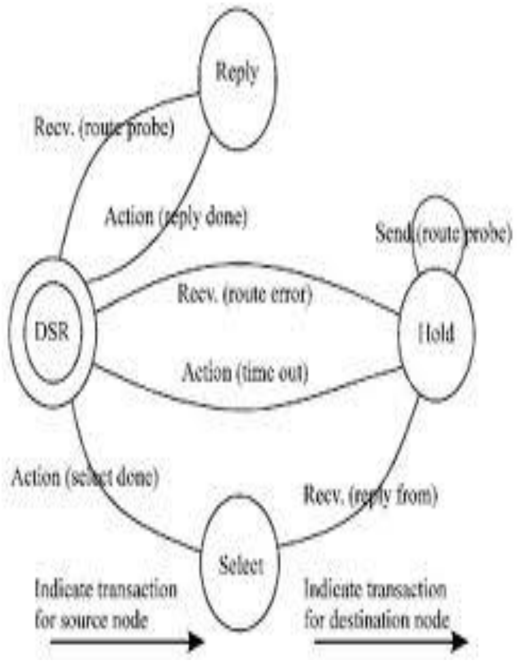


Fig. 1.2: DSR route request reply

AODV

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination. The connection setup delay is lower. One disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead. Another disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing.

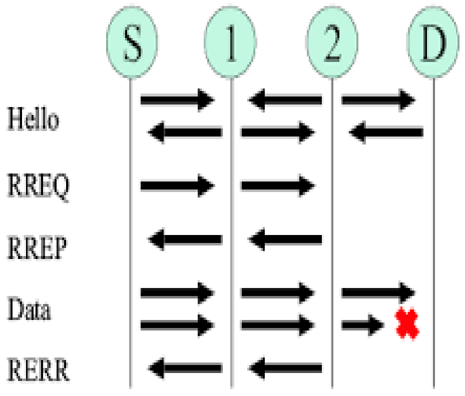


Fig. 1.3: message passing in AODV

DSR Vs AODV

a. DSR has less routing overhead than AODV.
b. AODV has less normalized MAC overhead than DSR.
c. DSR is based on a source routing mechanism whereas AODV uses a combination of DSR and DSDV mechanisms.
d. AODV has better performance than DSR in higher-mobility scenarios.
e. DSR has less frequent route discovery processes than AODV.

II. MECHANISM USED FOR SECURITY

RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

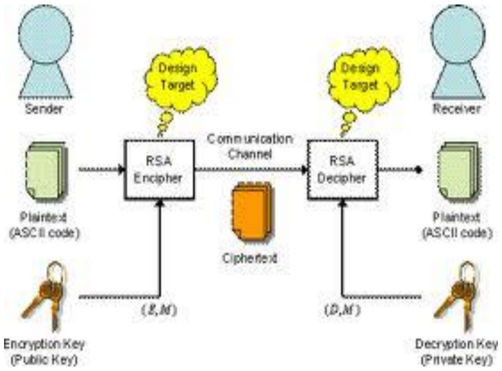


Fig. 1.4: RSA Algorithm

Diffie Hellaman Algorithm

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

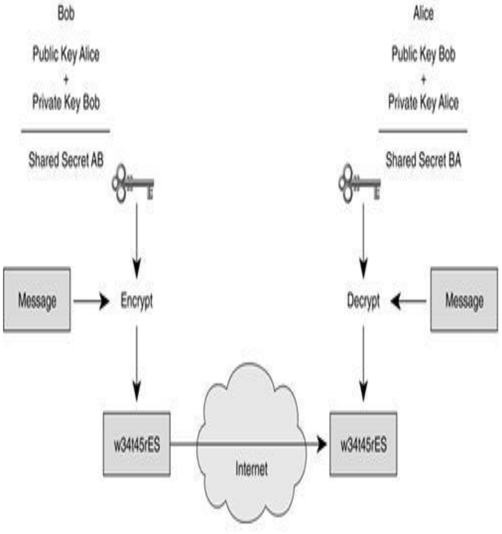


Fig. 1.5: Diffe Hellman Algorithm

Onion Routing

Onion routing is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of the vegetable onion. The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

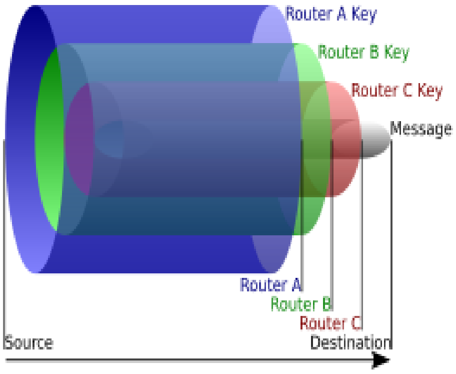


Fig. 1.6: Onion Routing

An onion is the data structure formed by "wrapping" a message with successive layers of encryption to be decrypted ("peeled" or "unwrapped") by as many intermediary computers as there are layers before arriving at its destination. The original message remains hidden as it is transferred from one node to the next, and no intermediary knows both the origin and final destination of the data, allowing the sender to remain anonymous.

Group Signature

A Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group.

basic requirements:

a. Soundness and Completeness: Valid signatures by group members always verify correctly, and invalid signatures always fail verification.
b. Unforgivable: Only members of the group can create valid group signatures.
c. Anonymity: Given a message and its signature, the identity of the individual signer cannot be determined without the group manager's secret key.
d. Traceability: Given any valid signature, the group manager should be able to trace which user issued the signature. (This and the previous requirement imply that only the group manager can break users' anonymity.)
e. Unlinkability: Given two messages and their signatures, we cannot tell if the signatures were from the same signer or not.

III. ANONYMOUS PROTOCOL FOR MANET

An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks.

A Secure Onion Throat (SOT) protocol is proposed to provide complete anonymity in an adverse environment. The SOT protocol is designed based on the combination of group signature and onion routing with ID-based encryption for route discovery.

MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks.

DOI 10.17148/IJARCCE.2015.45110

The shared wireless medium of mobile ad hoc networks facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. Termed MASK, which can accomplish both MAC-layer and network-layer communications without disclosing the real ID's of the participating nodes.

ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. Mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations.

IV. TYPES OF ATTACK IN NETWORK

Active Attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

Types of active attacks:

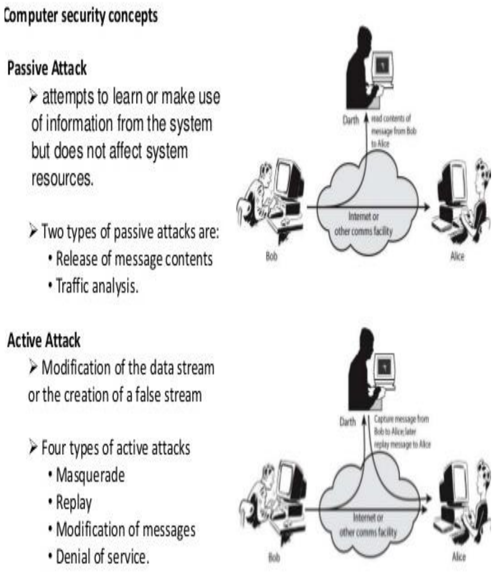
a. In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.
b. In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.
c. In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.
d. In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

Passive Attack

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

Types of passive attack

a. Wiretapping: Telephone tapping is the monitoring of telephone and Internet conversations by a third party, often by covert means. The wire tap received its name because, historically, the monitoring connection was an actual electrical tap on the telephone line. Legal wiretapping by a government agency is also called lawful interception. Passive wiretapping monitors or records the traffic, while active wiretapping alters or otherwise affects it
b. Port scanner: A port scan or port scan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service, however the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.
c. Idle scan: The idle scan is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer called a "zombie" (that is not transmitting or receiving information) and observing the behaviour of the "zombie" system.


Computer security concepts

Passive Attack
- attempts to learn or make use of information from the system but does not affect system resources.
- Two types of passive attacks are:
  - Release of message contents
  - Traffic analysis.

Active Attack
- Modification of the data stream or the creation of a false stream
- Four types of active attacks
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service.

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Fig. 1.7: Types of attacks

5. CONCLUSIONS

In this paper, we have tried to bring out in general the concept of mobile ad hoc network (MANETs), Security issues, and types of attacks in the network and how to overcome it. With the help of mechanisms used such as group signature, onion routing, etc.

REFERENCES

[1]. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888– 902, Aug. 2007

[2]. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.

[3]. Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006

[4]. K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Trans. on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

DOI 10.17148/IJARCCE.2015.45110