SECURITY

NETWORK SECURITY REQUIREMENTS

A security protocol for ad hoc wireless networks should satisfy the following requirements

1. *Confidentiality:*
   a. The data sent by the sender must be comprehensible only to the intended receiver.
   b. Though an intruder might get hold of the data being sent, he / she must not be able to derive any useful information out of the data.
   c. One of the popular techniques used for ensuring confidentiality is *data encryption.*

2. *Integrity:*
   a. The data sent by the source node should reach the destination node without being altered.
   b. It should not be possible for any malicious node in the network to tamper with the data during transmission

3. *Availability:*
   a. The network should remain operational all the time.
   b. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it.
   c. It should be able to provide guaranteed services whether an authorized user requires them

4. *Non-Repudiation:*
   a. It is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
   b. *Digital signatures* are used for this purpose.

ISSUES AND CHALLENGES IN SECURITY PROVISIONING

1. *Shared broadcast radio channel :*
   a. The radio channel used for communication in adhoc wireless networks is broadcast in nature & is shared by all nodes within its direct transmission range.
   b. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network.
   c. This problem can be minimized to a certain extent by using *directional antennas.*

2. *Limited resource availability :*
   a. Resources such as bandwidth, battery power, & computational power are scarce in adhoc wireless networks.
   b. Hence it is difficult to implement complex cryptography-based security mechanisms in networks.

3. *Insecure operational environment :*
   a. The operating environments where adhoc wireless is used may not always be secure.
   b. One important application of such networks is in battlefields.

4. *Physical Vulnerability :*
   a. Nodes in these networks are usually compact & hand-held in nature.
   b. They could get damaged easily & are also vulnerable to theft.

5. *Lack of central authority :*
   a. In wired networks & infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points & implement security mechanisms at such points.
   b. Since adhoc –wireless networks do not have central points, these mechanisms cannot be applied in ad hoc wireless networks.

6. *Lack of associations:*
   a. Since these networks are dynamic in nature, a node can join or leave the network at any pont oftime.
   b. If no proper authentication mechanism is used for associating nodes in a network, an intruder would be able to join into the network quite easily & carry out his/her attacks.

NETWORK SECURITY ATTACKS

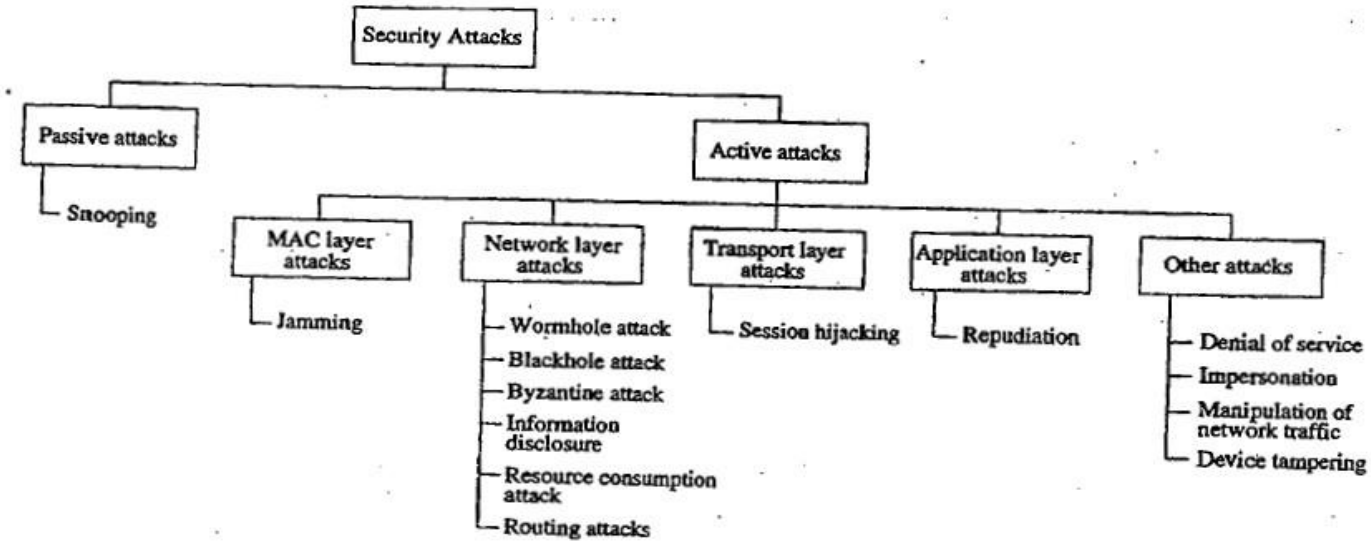

Figure 9.11. Classifications of attacks.

Attacks on adhoc wireless networks can be classified into 2 broad categories, namely:

1. *Passive attack*
   a. It does not disrupt the operation of the network; the adversary snoops the data exchanged inthe network without altering it.
   b. One way to overcome such problems is to use powerful encryption mechanisms to encrypt the data being transmitted.

2. *Active attack*
   a. An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.
   b. They can be further classified into 2 categories :
      i. External attacks, which are carried out by nodes that do not belong to the network. Theycan be prevented using standard encryption techniques and firewalls.
      ii. Internal attacks are from compromised nodes that are actually part of the network.

NETWORK LAYER ATTACKS

There are many types of attacks pertaining to the network layer in network protocol stack. Some of them are as follows:

1. ***Wormhole attack:***
    a. In this attack, an attacker receives packets at one location in the network & tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. This tunnel between 2 colliding attackers is referred to as a wormhole.
    b. If proper mechanisms are not employed to defend the network against wormhole attacks, existing routing protocols for adhoc wireless networks may fail to find valid routes.

2. ***Blackhole attack:***
    a. In this attack, a malicious node falsely advertises good paths to destination node during path- finding process or in route update messages.
    b. The intention of malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node.

3. ***Byzantine attack:***
    a. Here, a compromised intermediate note or a set of compromised intermediate nodes work in collusion & carries out attack such as creating routing loops, routing packets on non-optimal paths & selectively dropping packets.

4. ***Information disclosure:***
    a. A compromised node may leak confidential or important information to unauthorized nodes in the network.

5. ***Resource consumption attack:***
    a. In this attack, a malicious node tries to consume/waste resources of other nodes present in the network.
    b. The resources targeted are battery power, bandwidth & computational power, which are limitedly available in adhoc wireless networks.

6. ***Routing attacks:***
    a. There are several types of attacks mounted on routing protocol & they are as follows:
        i. *Routing table overflow:*
            - In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.
            - The main objective of this attack is to cause an overflow of routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.
        ii. *Routing table poisoning*:
            - Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.
            - This may result in sub-optimal routing, congestion in network or even make some parts of network inaccessible.
        iii. *Packet replication:*
            - In this attack, an adversary node would replicate state packets.
        iv. *Route cache poisoning:*

- Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar activities.

v. *Rushing attack:*

- On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

TRANSPORT LAYER ATTACKS:

1. *Session Hijacking:*
   a. Here, an adversary takes control over a session between 2 nodes.
   b. Since most authentication processes are carried out only at the start of session, once the sessionbetween 2 nodes get established, the adversary node masquerades as one of the end-nodes of the session & hijacks the sessions.

APPLICATION LAYER ATTACKS:

1. *Repudiation:*
   a. It refers to the denial or attempted denial by a node involved in a communication of havingparticipated in all or part of the communication

OTHER ATTACKS:

This section discusses security attacks that cannot strictly be associated with any specific layer in the network protocol stack

MULTI-LAYER ATTACKS

Multi-layer attacks are those that could occur in any layer of the network protocol stack. Some of the multi- layer attacks in adhoc wireless networks are:

1. Denial of Service

- In this type of attack, an adversary attempts to prevent legitimate & authorized users of services offered bythe network from accessing those services.
- This may lead to a failure in the delivery of guaranteed services to the end users.
- Some of the DoS attacks are as follows:
  - **Jamming** – in this form of attack, the adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. Frequency hopping spread spectrum(FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks
  - **SYN flooding** – here, an adversary sends a large number of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The victim node builds up a table/data structure for holding information regarding all pending connections. Since the maximum possible size of the table is limited, the increasing number of half-connections results in an overflow in the table.
  - **Distributed DoS attack** – here, several adversaries that are distributed throughout the network collide and prevent legitimate users from accessing the services offered by the network.

2. Impersonation

- In these attacks, an adversary assumes the identity & privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network by injecting false routing information into the network.
- A *man-in-the-middle* attack is another type of impersonation attack.

DEVICE TAMPERING

- Unlike nodes in a wired network, nodes in adhoc wireless networks are usually compact, soft and hand- held in nature.
- They could get damaged or stolen easily.

KEY MANAGEMENT

Having seen the various kinds of attacks possible on adhoc wireless networks, we now look at various techniques employed to overcome the attacks.

- **CRYPTOGRAPHY** is one of the most common & reliable means to ensure security & can be applied toany communication network.
- In the parlance of cryptography, the original information to be sent from one person to another is called plaintext.
- The plaintext is converted into ***ciphertext*** by the process of ***encryption.***
- An authentic receiver can decrypt / decode the ciphertext back into plaintext by the process of decryption.
- The process of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the keys is to be kept secret to ensure the security of the system, it is called a ***secret key.***
- The secure administration of cryptographic keys is called ***Key Management.***
- The 4 main goals of cryptography are confidentiality, integrity, authentication & non-repudiation.
- There are 2 major kinds of cryptographic algorithms:
    1. ***Symmetric*** *key algorithms*, which use the same key for encryption & decryption.
    2. ***Asymmetric*** *key algorithms*, which use two different keys for encryption & decryption.

The asymmetric key algorithms are based on some mathematical principles which make it feasible or impossible to obtain one key from another; therefore, one of the keys can be made public while the others is kept secret (private). This is called public key cryptography

SYMMETRIC KEY ALGORITHMS

- Symmetric key algorithms rely on the presence of shared key at both the sender & receiver, which has been exchanged by some previous arrangement.
- There are 2 kinds of symmetric key algorithms:
    - One involving block ciphers &
    - The stream ciphers.
- A block cipher is an encryption scheme in which plaintext is broken into fixed-length segments called blocks, & the blocks are encrypted one at a time.
- The simplest example includes substitution & transposition.
- In *substitution,* each alphabet of plaintext is substituted by another in the cipher text,& this tablemapping of the original & the substituted alphabet is available at both the sender & receiver.
- A *Transposition cipher,* permutes the alphabet in plaintext to produce the cipher text.

Refer Fig 9.12 Substitution and transposition from textbook (page no: 438)

ASYMMETRIC KEY ALGORITHMS

- Asymmetric key (or public key) algorithms use different keys at the sender end & receiver ends for encryption & decryption, respectively.
- Let the encryption process be represented by a function E, & decryption by D. Then plaintext 'm' is transformed into the ciphertext 'c' as

  $$C = E(m)$$

  The receiver then decodes c by applying D. Hence, D is such that $m = D(c) = D(E(m))$
- When this asymmetric key concept is used in public key algorithms, the key E is made public, while D is made private, known only to the intended receiver.
- RSA algorithm is the best example of public key cryptography.
- Digital signatures scheme are also based on public key encryption.
- These are called reversible public key systems
- In this case, the person who wishes to sign a document encrypts it using his/her private key D, which is known only to him/her.
- Anybody who has his/her public key E can decrypt it and obtain the original document
- A trusted third party is responsible for issuing these digital signatures and for resolving any disputes regarding the signatures
- This is usually a governmental or business organization

KEY MANAGEMENT APPROACHES

- The primary goal of key management is to share a secret (some information) among a specified set of participants.
- The main approaches to key management are key predistribution, key transport, key arbitration and key agreement.

1. KEY PREDISTRIBUTION:

- Key predistribution, as the name suggests, involves distributing key to all interested parties before the start of communication.
- This method involves much less communication & computation, but all participants must be known *a priori*, during the initial configuration.
- Once deployed, there is no mechanism to include new members in the group or to change the key.
- As an improvement over predistribution scheme, sub-groups may be formed within a group, and some communication may be restricted to a subgroup.
- However, formation of subgroups is also an *a priori* decision.

2. KEY TRANSPORT:

- In key transport systems, one of the communicating entities generates keys & transports them to the other members.
- The simplest scheme assumes that a shared key already exists among the participating members. This shared key is used to encrypt a new key & is transmitted to all corresponding nodes.
- Only those nodes which have the prior shared key can decrypt it.
- This is called the *Key Encrypting Key (KEK) method.*

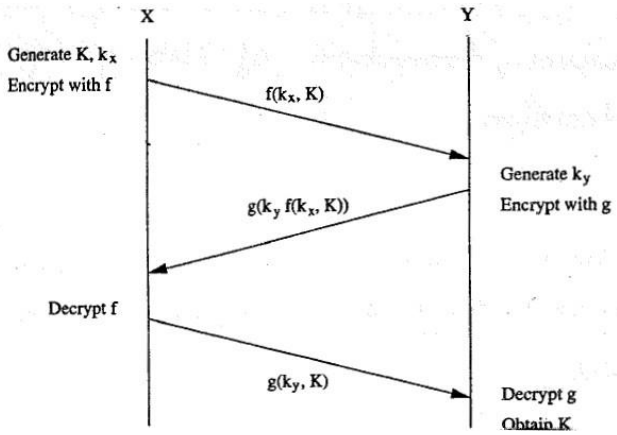

Figure: Shamir's three-pass protocol

An interesting method for key transport without prior shared keys is the shamir's three-pass protocol.The scheme is based on a special-type of encryption called communicative Encryption schemes.

Consider 2 nodes X & Y which wish to communicate. Node X selects a key K which it wants to use in its communication with node Y.It then generates a random key K_X ,using which it encrypts K with f, & sends to node Y. Node Y encrypts this with a random key k_Y using g,& sends this back to node X.

Now, node X decrypts this message with its key K_X, & after applying inverse function f^{-1},sends it to node y. finally, node Y decrypts the message using Ky & g^{-1} to obtain key K.

3. KEY ARBITRATION:

- Key arbitration schemes use a central arbitrator to create & distribute keys among all participants.
- Hence, they are a class of key transport schemes.
- In ad hoc wireless networks, the problem with implementation of arbitrated protocols is that thearbitrator has to be powered on at all times to be accessible to all nodes
- This leads to a power drain on that particular node
- Alternative is to make the keying service distributed
- If any one of the replicated arbitrators is attacked, the security of the whole system breaks down

4. KEY AGREEMENT:

- Key agreement protocols are used to establish a secure context over which a session can be run,starting with many parties who wish to communicate & an insecure channel.
- In group key agreement schemes, each participant contributes a part to the secret key.
- Require least amount of preconfiguration
- Have high computational capability
- The most popular key agreement schemes use the Diffie-Hellman exchange, an asymmetric key algorithm based on discrete logarithms.

KEY MANAGEMENT IN ADHOC WIRELESS NETWORKS

- Adhoc wireless networks pose certain specific challenges in key management, due to the lack of infrastructure in such networks.
- 3 types of infrastructure have been identified, which are absent in adhoc wireless networks:
  - The first is the network infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes.
  - The second missing infrastructure is services, such as name resolution, directory & TTP's.
  - The third missing infrastructure in adhoc wireless network is the administrative support of certifyingauthorities.

Password-Based Group Systems:

- A password-based system has been explored where, in the simplest case, a long string is given as thepassword for users for one session.
- However, human beings tend to favour natural language phrases as passwords, over randomlygenerated strings.
- Such passwords, if used as keys directly during a session, are very week & open to attack directly during a high redundancy, & the possibility of reuse over different sessions.
- Hence, protocols have been proposed to derive a strong key (not vulnerable to attacks).
- This password-based system could be two-party, with a separate exchange between any 2 participants, or it could be for the whole group, with a leader being elected to preside over the session.
- The protocol used is as follows :
  - Each participant generates a random number, & sends it to all others.
  - When every node has received the random number of every other node, a common pre-decidedfunction is applied on all the numbers to calculate a reference value.
  - The nodes are ordered based on the difference between their random number & the referencevalue.

Threshold Cryptography:

- Public Key Infrastructure (PKI) enables the easy distribution of keys & is a scalable method.
- Each node has a public/private key pair,& a certifying authority (CA) can bind the keys to a particular node. But CA has to be present at all times, which may not be feasible in Adhoc wireless networks.
- A scheme based on threshold cryptography has been proposed by which n servers exist in an adhoc wireless network, out of which any (t+1) servers can jointly perform arbitration or authorization successfully, but t servers cannot perform the same. This is called an (n, t+1) configuration, where n >= 3t +1.
- To sign a certificate, each server generates a partial signature using its private key & submits it to a combiner. The combiner can be any one of the servers.
  - In order to ensure that the key is combined correctly, t+1 combiners can be used to account forat most t malicious servers.
  - Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.
  - If verification fails, it means that at least one of the t+1 keys is not valid, so another subset of t+1 partial signature is tried. If combiner itself is malicious, it cannot get a valid key, because partial key itself is always invalid.

Self-Organised Public Key Management for Mobile Adhoc Networks:

- Self-organised public key system makes use of absolutely no infrastructure.
- The users in the adhoc wireless network issue certificates to each other based on personal acquaintance.

- A certificate is binding between a node & its public key. These certificates are stored & distributed by the users themselves. Certificates are issued only for specific period of time, before it expires; the certificate is updated by the user who had issued the certificate.
- Each certificate is initially stored twice, by the issuer & by the person for whom it is issued.
- If any of the certificates are conflicting (e.g: the same public key to different users, or the same user having different pubic keys), it is possible that a malicious node has issued a false certificate.
- A node then enables such certificates as conflicting & tries to resolve the conflict.
- If the certificates issued by some node are found to be wrong, then that node may be assumed to be malicious.
- A certificate graph is a graph whose vertices are public keys of some nodes and whose edges are public key certificates issued by users.

SECURE ROUTING IN AD HOC WIRELESS NETWORKS

Ensuring secure communication in adhoc wireless networks include the mobility of nodes, a promiscuous mode of operation, limited processing power & limited availability of resources such as battery power, bandwidth & memory.

REQUIREMENTS OF A SECURE ROUTING PROTOCOL FOR ADHOC WIRELESS NETWORKS

The fundamental requirements for a secure routing protocol for adhoc wireless networks are listed as below:

- Detection of malicious nodes:
  - A secure routing protocol should be able to detect the presence of any malicious node in thenetwork & should avoid the participation of such nodes in the routing process.
- Guarantee of correct route discovery:

If a route between the source & destination node exist, the routing protocol should be able tofind the route, & should also ensure the correctness of the selected route.

- Confidentiality of network topology:
  - Once the network topology is known, the attacker may try to study the traffic pattern in the network. If some of the nodes are found to be more active compared to others, the attacker may try to mount attacks.
  - This may ultimately affect the ongoing routing process. Hence, confidentiality of network topology is important.
- Stability against attacks:
  - The routing protocols must be self-stable in the sense that it must be able to revert to its normal operating state within a finite amount of time after passive or an active attack.
  - Some of the security-aware routing protocols proposed for adhoc wireless networks are discussed.

SECURITY AWARE ADHOC ROUTING PROTOCOL

- This routing protocol uses security as one of the key metrics in path finding.
- In adhoc wireless networks, communication between end nodes through possibly multiple intermediate nodes is based on the fact that the two end nodes trust the intermediate nodes.
- SAR defines level of trust as a metric for routing & as one of the attributes for security to be taken into consideration while routing.
- The routing protocol based on level of trust is explained in below figure.

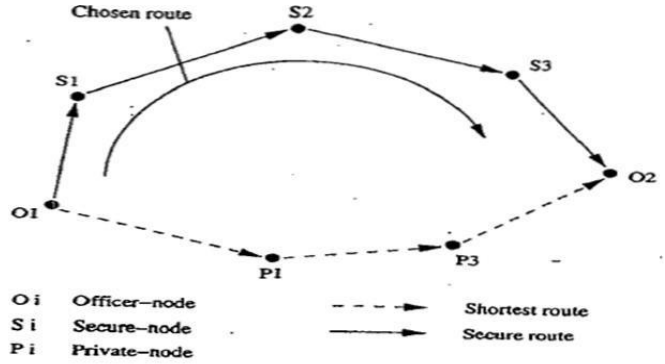

Figure 9.14. Illustration of the level of trust metric.

- Two paths exist between the two officers O1 and O2 who want to communicate with each other
- One of these paths is a shorter path which runs through private nodes whose trust levels are very low
- Hence, the protocol chooses a longer but secure path which passes through other secure nodes
- Nodes of equal levels of trust distribute a common key among themselves and with those nodes havinghigher levels of trust
- The SAR mechanism can be easily incorporated into the traditional routing protocols for ad hoc wireless networks
- It could be incorporated into both on-demand and table-driven routing protocols
- The SAR protocol allows the application to choose the level of security it requires
- But the protocol requires different keys for different levels of security
- This tends to increase the number of keys required when the number of security levels used increase

SECURE EFFICIENT AD HOC DISTANCE VECTOR ROUTING PROTOCOL

- SEAD routing protocol is a secure ad hoc routing protocol based on the destination-sequenced distance vector (DSDV) routing protocol
- This protocol is mainly designed to overcome security attacks such as DoS and resource consumption attacks
- The protocol uses a one-way hash function and does not involve any asymmetric cryptographicoperation

DISTANCE VECTOR ROUTING

Distance vector routing protocols belong to the category of table-driven routing protocols

- Each node maintains a routing table containing the list of all known routes to various destination nodes in the network
- The metric used for routing is the distance measured in terms of hop-count
- The routing table is updated periodically by exchanging routing information
- An alternative approach to this is triggered updates, in which each node broadcasts routing updates only if its routing table gets altered.

ONE-WAY HASH FUNCTION

- SEAD uses authentication to differentiate between updates that are received from non-malicious nodes and malicious nodes
- This minimizes resource consumption attacks caused by malicious nodes
- SEAD uses a one-way hash function for authenticating the updates
- A one-way hash function (H) generates a one-way hash chain (h1, h2,).
- The function H maps an input bit-string of any length to a fixed length bit-string
- To create a one-way hash chain, a node generated a random number with initial value x € (0,1)p, where p is the length in bits of the output bit-string
- h0 is the first number in the has chain is initialised to x
- The remaining values are computed using a general formula hi = H(hi-1) for $0 \leq i \leq n$, for some n.
- SEAD avoids routing loops unless the loop contains more than one attacker
- The protocol is robust against multiple coordinated attacks
- SEAD protocol would not be able to overcome attacks where the attacker uses the same metric and sequence number which were used by the recent update message, and sends a new routing update

AUTHENTICATED ROUTING FOR AD HOC NETWORKS

- ARAN is a secure routing protocol which successfully defeats all identified attacks in the network layer
- It takes care of authentication, message integrity and non-repudiation
- During the route discovery process of ARAN, the source node broadcasts RouteRequest packets
- Destination packets responds by unicasting back a reply packet on the selected path
- The ARAN protocol uses a preliminary cryptographic certification process, followed by an end-to-end route authentication process, which ensures secure route establishment

ISSUE OF CERTIFICATES

- There exists an authenticated trusted server whose public key is known to all legal nodes in thenetwork
- The ARAN protocol assumes that keys are generated a priori by the server and distributed to all nodes in the network
- On joining the network, each node receives a certificate from the trusted server
- The certificate received by a node A from the trusted server T looks like the following:

$$T \rightarrow A: \ cert_A = [IP_A, K_{A+}, t, e]K_{T-} \qquad (9.12.1)$$

Here, IP_A, K_{A+}, t, e, and K_{T-} represent the IP address of node A, the public key of node A, the time of creation of the certificate, the time of expiry of the certificate, and the private key of the server, respectively.

END-TO-END ROUTE AUTHENTICATION

- The main goal of this end-to-end route authentication process is to ensure that the correct intended destination is reached by the packets sent from the source node
- The source node *S* broadcasts a *RouteRequest/RouteDiscovery* packet destined to destination node *D*.

$$S \rightarrow broadcasts := [RDP, IP_D, Cert_S, N_S, t]K_{S-}$$
$$A \rightarrow broadcasts := [[RDP, IP_D, Cert_S, N_S, t]K_{S-}]K_{A-}, Cert_A$$
$$D \rightarrow X := [REP, IP_S, Cert_D, N_S, t]K_{D-}$$

Where,

K_{A+}	Public key of node A.
K_{A-}	Private key of node A.
K_{AB}	Symmetric key shared by nodes A and B.
$\{d\}K_{A+}$	Encryption of data d with key K_{A+}.
$[d]K_{A-}$	Data d digitally signed by node A.
cert_A	Certificate belonging to node A.
e	Certificate expiration time.
N_A	Nonce issued by node A.
IP_A	IP address of node A.
RDP	Route Discovery Packet identifier.
REP	REPly packet identifier.
t	timestamp.

Table 9.3. Comparison of vulnerabilities of ARAN with DSR and AODV protocols

Attacks	Protocols		
	AODV	DSR	ARAN
Modifications required during remote redirection	Sequence number and hop-counts	Source routes	None
Tunneling during remote redirection	Yes	Yes	Yes
Spoofing	Yes	Yes	No
Cache poisoning	No	Yes	No

SECURITY AWARE AODV PROTOCOL

- AODV is an on-demand routing protocol where the route discovery process is initiated by sending RouteRequest packets only when data packets arrive at a node for transmission
- A malicious intermediate node could advertise that it has the shortest path to the destination, thereby redirecting all the packets through itself
- This is known as black hole attack

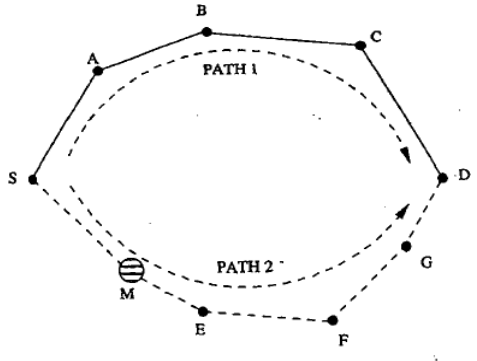

Figure 9.15. Illustration of blackhole problem.

- Let node M be the malicious node that enters the network
- It advertises that it has the shortest path to the destination node D when it receives the RouteRequest packet sent by node S
- The attacker may not be able to succeed if node A, which also receives the RouteRequest

packet from node S, replies earlier than node M

- Advantage malicious node does not have to search its routing table for a route to the destination
- Hence the malicious node would be able to reply faster than node A

SOLUTIONS FOR THE BLACK HOLE PROBLEM

- One of the solutions for the blackhole problem is to restrict the intermediate nodes from originating RouteReply packets
- Only the destination node would be permitted to initiate RouteReply packets

Security is not completely assured.

- The delay involved in the route discovery process increases as the size of the network increases

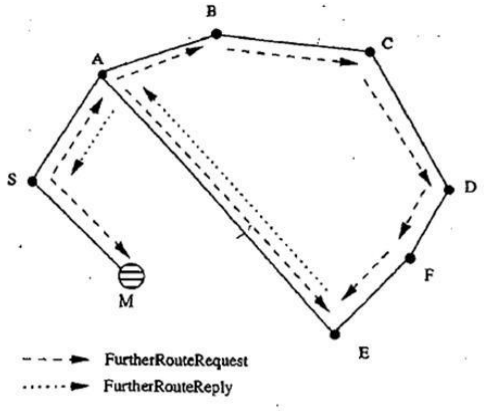

Figure 9.16. Propagation of *FurtherRouteRequest* and *FurtherRouteReply*.

- The source node S sends FurtherRouteRequest packets to this neighbour node E
- Node E responds by sending a FurtherRouteReply packet to source node S
- Since node M is a malicious node which is not present in the routing list of node E, theFurtherRouteReply packet sent by node E will not contain a route to the malicious node M.
- This protocol completely eliminates the blackhole attack caused by a single attacker
- Disadvantage control overhead of the routing protocol increases considerably
- If the malicious nodes work in a group, this protocol fails miserably.