NETWORK SECURITY FOR MANET: A SURVEY

[1]Amirthasaravanan.A, [1]Sridevi.N, [2]Monica.N, [3] Pazhaniraja.N

[12,3]Department of Information Technology,
[1]University College of Engineering Villupuram,
Villupuram,India.
[2]KSR Institute for Engineering and Technology,
Tiruchengode,Namakkal,India.
Sri Manakula Vinayagar Engineering College
Puducherry.india.

E-mail: aasaravanan777@gmail.com , sridevi.792@gmail.com, nmonica915@gmail.com,pazhanibit@gmail.com

ABSTRACT - ***We present a survey of secure ad hoc routing protocols for wireless networks. Ad hoc network is an assortment of nodes that connected through a wireless medium forming swiftly changing topologies. The emerging attacks on ad hoc network routing protocols disrupt network performance and reliability with their solution. We present the most popular and effective protocols that follow the table-driven and the source-initiated on-demand approaches. The evaluation between the proposed solutions and parameters of ad hoc network shows the performance according to secure protocols. We present a survey paper on routing protocol and it's confront .we also discuss authentication in ad hoc network for effective MANET.***

Keywords: Table-driven, Source-initiated, On-Demand Approaches

1. INTRODUCTION

Wireless networks consist of a number of nodes, which communicate with each other over a wireless channel which have assortment types of networks: sensor network, ad hoc mobile network, and cellular network and satellite networks. Wireless sensor networks consist of small nodes with sensing, computation and wireless communications competence. Many routing protocols have been specifically designed for WSNs where energy awareness is the key issue. Routing protocols in WSNs diverge depending on the application and network architecture. Ad-hoc networks are a new pattern of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support moveably and classify themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and capriciously. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server infrastructure. Without support from the fixed infrastructure, it is indubitably arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegitimate participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical confront when we design a wireless network system. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely elastic technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster condition.

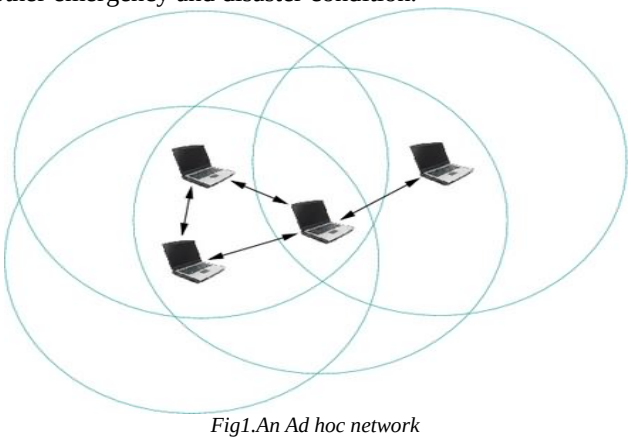

Fig1.An Ad hoc network

Since, all nodes are mobile; the network topology of a MANET is generally dynamic and may vary frequently. Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, direct *single-hop* transmissions between two hosts can require significant power, causing interference with other such communication. To avoid this *routing problem*, two hosts can use *multi-hop* transmission to communicate via other hosts in the network A router should provide the ability to rank routing information sources from most trustworthy to least reliable and to accept routing information about any particular destination from the most trustworthy sources first.

A router should provide a mechanism to filter out obviously invalid routes. Routers must not by default redistributes routing data they do not themselves use, trust or otherwise consider valid. Routers must be at least a little paranoid about accepting routing data from anyone, and must be especially cautious when they distribute routing information provided to them by another party. Figure 1 show four nodes where ad hoc network where every node connected to wireless, and work as access point to forward and receive data. This article discusses attacks on ad hoc networks and discusses current approaches for establishing cryptographic keys in ad hoc networks. We portray the state of research in secure ad hoc routing protocols, routing confronts and its research issues.

2. ROUTING PROTOCOL AND ITS CHALLENGE IN AD HOC NETWORK

In this section, we are going to discuss different approaches adopted for routing and security challenges in Ad hoc networks.

2.1 ROUTING PROTOCOLS

Routing in mobile ad hoc networks faces additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. Several well-known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. Most of the existing routing protocols follow two different design approaches to confront the inherent Characteristics of ad hoc networks: the *table-driven* and the *source-initiated on-demand* approaches. Table-driven ad hoc routing protocols maintain at all times routing information regarding the connectivity of every node to all other nodes that participate in the network. Also known as *proactive*, these protocols allow every node to have a clear and consistent view of the network topology by propagating periodic updates. An alternative approach to that followed by table-driven protocols is the source-initiated on-demand routing. According to this approach, a route is formed only when the source node requires a route to a specific destination. A route is obtained by the initiation of a *route discovery* function by the source node.

The data packets transmitted while a route discovery is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required through a *route maintenance* procedure. Table 1 shows the various types of routing protocols according to Parameter which are response times, bandwidth energy.

TABLE 1: Classification of routing protocol

Parameter	Network	Protocols
Response Time And Bandwidth	Ad hoc	Proactive protocols
		Reactive protocols
Energy	Sensor	Network structure
		Protocol operation

2.2 SECURITY CHALLENGES IN AD HOC NETWORKS

Use of wireless links renders an Ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion [9].Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting flawed messages; impersonate a node etc thus breach availability, integrity, authentication and no repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from exterior but also from within the network from compromised nodes.

Thus following are the traditions by which security can be breached.

2.2.1 Vulnerability of Channels: As in any wireless network, messages can be eavesdropped and forged messages can be injected into the network without the difficulty of having physical access to network components.

2.2.2 Vulnerability of nodes: Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be detain and fall under the control of an attacker.

2.2.3 Absence of Infrastructure: Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the traditional security solutions based on certification authorities and on-line servers inapplicable.

2.2.4 Dynamically Changing Topology: In mobile ad hoc networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an supplementary challenge. A particular difficulty is that wrong routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases. For high survivability Ad hoc networks must have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to common changes in topology. Even the trust relationships among individual nodes also changes, particularly when some nodes are found to be compromised. Security mechanism needs to be on the dynamic and scalable not being static.

3. SECURITY MODEL

In this section we first discuss security goals attacks and thus secure routing protocol which are following,

3.1 SECURITY GOALS FOR AD HOC

3.1.1 Availability: Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming practice to interfere with communication on physical channel. On network layer the attacker can disturb the routing protocol. On higher layers, the attacker could defeat high level services e.g.: key management service.

3.1.2 Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

3.1.3 Integrity: Message being transmitted is never tarnished.

3.1.4 Authentication: Enables a node to guarantee the identity of the peer node it is communicating with. Without which an attacker would imitate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

3.1.5 Non-repudiation: Ensures that the origin of a message cannot contradict having sent the message.

3.1.6 Non-impersonation: No one else can pretend to be another authorized member to study any useful information.

3.1.7 using fabrication: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to identify.

3.2 ATTACKS ON AD HOC NETWORK

There are different types of attacks on ad hoc network which are describing following:

3.2.1 Location Disclosure: Location discovery is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques, or with simpler inquisitive and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

3.2.2 Black Hole: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a target. These fake replies can be fabricated to deflect network traffic through the malicious node for eavesdropping, or just to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

3.2.3 Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured earlier. This attack usually targets the freshness of routes, but can also be used to challenge poorly designed security solutions.

3.2.4 Wormhole: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that contribute in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that distribute a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is entirely under the control of the two colluding attackers. The solution to the wormhole attack is *packet leashes*.

3.2.5 Blackmail: This attack is relevant against routing protocols that use mechanisms for the classification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate genuine nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it connect a node to the messages it generated.

3.2.6 Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the complete operations of the ad hoc network. Specific instances of denial of service attacks include the *routing table overflow and sleep deprivation torture.* In a routing table overflow attack the malicious node floods the network with fake route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the utilization of batteries of a specific node by constantly keeping it engaged in routing decisions.

3.2.7 Routing Table Poisoning: Routing protocols maintain tables that embrace information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify genuine messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the formation of routing loops, bottlenecks, and even portioning certain parts of the network.

3.2.8 Rushing Attack: Rushing attack is that results in denial-of-service when used in opposition to *all* previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Aridne, ARAN, and SAODV, are not capable to discover routes longer than two hops when subject to this attack. develop *Rushing Attack Prevention (RAP),* a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to defend against the rushing attack.

3.2.9 Breaking the neighbor relationship: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even interrupt traffic belonging to any data session.

3.2.10 Masquerading: During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and dishonestly joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a negotiation IS.

3.2.11 Passive Listening and traffic analysis: The intruder could passively gather uncovered routing information. Such an attack cannot effect the operation of routing protocol, but it is a violation of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the privacy of user data is not the responsibility of routing protocol

3.3 ROUTING SECURITY IN AD HOC NETWORK

The contemporary routing protocols for Ad hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocols capture

common security threats and provide guidelines to secure routing. Routers exchange network topology informally in order to establish routes between nodes another possible target for malicious attackers who mean to bring down the network. External attackers injecting invalid routing information, replaying old routing information, twist routing information in order to partition a network, or overloading a network with retransmissions and unproductive routing.

Internal compromised nodes - more severe detection and correction more difficult Routing information signed by each node won't work since compromised nodes can generate valid signatures using their private keys. Discovering of negotiation nodes through routing information is also difficult due to dynamic topology of Ad hoc networks. Routing protocols for Ad hoc networks must handle outdated routing information to accommodate dynamic changing topology. Bogus routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient numbers of valid nodes, the routing protocol must be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes between nodes. Routing protocol should be able to make use of an alternate route if the existing one appears to have faulted.

4. ROUTING AUTHENTICATION

Routing authentication is one of the important factors in ad hoc networks during route discovery because ad hoc is infrastructure less network. So it is necessary that a reply coming from a node against a route request must be authentic. That's why authentication protocol is required between the nodes of ad hoc network. In this section we emphasize on the ways by which these protocols can be use.

4.1 New key agreement scenario

Consider a group of people getting together for an Ad hoc meeting in a room and trying to set up a wireless network through their laptops. They belief one another personally; however don't have any a priori shared secret (password) to authenticate one another. They don't want anybody exterior the room to get a wind of their conversation indoors. This particular circumstances is vulnerable to any attacker who not only can monitor the communication but can also modify the messages and can also insert messages and make them emerge to have come from somebody inside the room. This is a typical example of Ad hoc network and the simplest way to tackle this example would be through location based key agreement - to map locations to name and then use identity based mechanisms for key agreement[10]. e.g.: participants writing the IP addresses on a piece of paper and passing it around. Then a certificate based key agreement mechanism can be used. These public key certificates can allow participants to verify the binding between the IP address and keys of other participants.

4.2 Two obvious problems

a) Difficult to determine if the certificate presented by the participant has been revoked.

b) Participants may be divided into 2 or more certification hierarchies and that they don't have cross certification hierarchies. One obvious solution A trusted third is party capable of locating players, however not always feasible due to no infrastructure nature of Ad hoc networks. Physically secure channel limited to those present in the room to negotiate the session key before switching to the insecure wireless channel.

4.3. Password based Authenticated Key Exchange

A fresh password is chosen and shared among those present in the room in order to capture the existing shared context. If this password is long random string, can be used to setup security organization, but less user friendly. Natural language phrases are more users friendly, however, Vulnerable to dictionary attacks [10]. Need to derive a strong session key from a weak shared password. Desirable properties for such a protocol are following,

4.3.1 Secrecy: Only those players that know the initial shared weak secret password should learn the session key and nobody else should.

4.3.2 Perfect Forward Secrecy: Warrants that if an attacker who succeeds in compromising one of the participants at a later time would be unable to figure out the session key resulting from previous runs of protocol.

4.3.3 Contributory Key Agreement: If each player participates in the creation of the final session key, by contributing, then it is called contributory key agreement.

4.3.4 Tolerance to Disruption Attempts: Not only strong attackers who can disrupt communication by jamming radio channels etc but even the weaker attackers who can insert but cannot modify or delete messages sent by players.

5. SECURE ROUTING PROTOCOLS

5.1 SEAD

Our Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network. To support use of SEAD with nodes of limited CPU processing capability and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use proficient one-way hash functions.

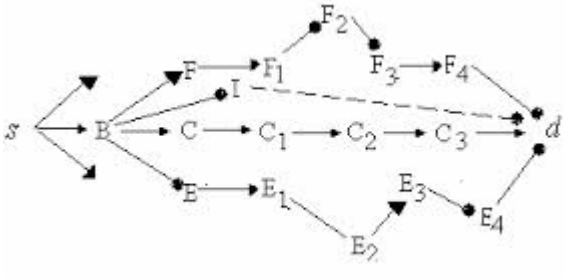

Fig2.Secure path

5.1.1 Hash chains*:* A one-way hash chain is built on a one-way hash function. Like a standard hash function, a one-way hash function *H* maps an input of any length to a fixed length bit string. Thus, *H*: {0,1}* _{0,1}p, where p _is the length in bits of the hash function's output. The function *H* should be simple to compute yet must be computationally infeasible in general to invert. To create a one-way hash chain, a node chooses a random *x* ∈ {0,1}p and computes the list of values *h*0, *h*1, *h*2, *h*3……*hn*, where *h*0= *x*, and *h*i = *H*(*h*i – 1) for 0 < *i* __*n*, for some *n*. The node at initialization generates the elements of its hash chain using this recurrence, in order of increasing subscript *i*; over time, it uses certain elements of the chain to secure its routing updates. In using these values, the node progresses in order of decreasing subscript i within the created chain. Given an existing authenticated element of a one way hash chain, we can verify elements later in the sequence of use within the chain (further on, in order of decreasing subscript). For example, given an authenticated *h*i value, a node can authenticate *h*i –3 by computing *H*(*H*(*H*(*h*i –3))) and verifying that the resulting value equals *h*i. To use one-way hash chains for authentication, we assume some mechanism for a node to distribute an authentic element such as *h*n from its generated hash chain.

5.2 SORP

SORP is a link state routing protocol used within one autonomous system (AS) or routing domain.

It creates a global network topology, which are following,

Phase I: Neighbor and Adjacency Establishment A router broadcasts periodically a Hello packet to discover its neighboring routers. After the neighboring routers establish connections, they synchronize their databases with each other through a Database Exchange Process.

Phase II: Information swapped by LSA Flooding A router assembles the link state information about its local neighborhood into a Link State Advertisement (LSA) and floods it to the whole network.

Phase III: Calculate Shortest Route using Link State Database After a router collects all the link state information,, it calculates a shortest path tree with itself as the root by using Dijkstra algorithm and forms a complete structure of routing in the network. OSPF divides an AS into groups of routers called *areas*.
A two level hierarchy among these areas is established, with the top level defined as the backbone area and the second level consisting of many areas attached to the backbone. Routers belonging to a single area are called *internal routers*. Routers that belong to more than one area

are called, Area Border Routers (ABR). All ABRs belong to the backbone and several of the routers, within an area or within the backbone, which exchange information with an external autonomous system, are known as Autonomous System Boundary Routers (ASBR). Security strong Points of OSPF routing protocol, some inherent properties of OSPF make it very robust to failures and some attacks.

5.2.1 Flooding And Information Least Dependency: As we mentioned above, OSPF uses flooding for the dissemination of LSAs. This makes sure that within the same *area* all the routers have the identical topological database. Even if a router goes down, other routers can still exchange their link state information provided that an alternate path exists. Furthermore, the link state information propagated in the network is the raw message generated by the original router instead of the summarized information from neighbors, which is the situation for distance vector routing. This makes it easy to protect the authenticity of the information.

5.2.2 Hierarchy routing and Information Hiding: OSPF is a two level routing protocol, which are intra-area routing & inter-area routing. ABRs connect to backbone and exchange summarized area information. Since intra-area routing depends only on information from within that area, it is not vulnerable to problems out of the area. And problems in one area will not influence the intra-area routing of other areas and inter-area routing among other areas. Therefore, hierarchy routing has security advantage.

5.3 SRP

Secure Routing Protocol [4] (Lightweight Security for DSR), which we can use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP does not attempt to secure ROUTE ERROR packets but instead delegates the route-maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. SRP uses a sequence number in the REQUEST to ensure freshness, but this sequence number can only be checked at the target. SRP requires a security association only among communicating nodes and uses this security association just to authenticate ROUTE REQUESTS and ROUTE REPLYS through the use of message authentication codes. At the target, SRP can detect modification of the ROUTE REQUEST, and at the source, SRP can detect modification of the ROUTE REPLY. Because SRP requires a security association only between communicating nodes, it uses extremely lightweight mechanisms to prevent other attacks. For example, to limit flooding, nodes record the rate at which each neighbor forwards ROUTE REQUEST packets and gives priority to REQUEST packets sent through neighbors that less frequently forward REQUEST packets. SRP authenticates ROUTE REPLYS from intermediate nodes using shared group keys or digital signatures. When a node with a cached route contribute to a group key with (or can generate a digital signature verifiable by) the initiator of the REQUEST, it can use that group key to authenticate the REPLYS. The authenticator, which is either a message authentication code, calculated using the group key or a signature is called the intermediate node reply token. The signature or MAC is calculated over the cache REPLY.

5.4 SECURE AODV

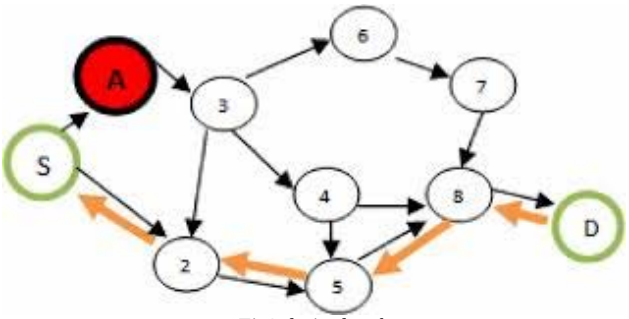

Fig3.desired path

The SecAODV implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the target, without any form of entrustment of trust. The SecAODV execution follows Tuominen's design, which uses two-kernel modules ip6_queue, ip6_nf_aodv, and a user space daemon AODV. The AODV daemon then produces a 1024-bit RSA key pair. Using the public key of this pair, the securely bound global and site-local IPv6 addresses are generated.

The AODV protocol is comprised of two basic mechanisms, route discovery, and maintenance of local connectivity. The SecAODV protocol adds security features to the basic AODV mechanisms, but is otherwise

identical. A source node that requests communication with another member of the MANET referred to as a destination D initiates the process by constructing and broadcasting a signed route request message RREQ. The format of the SecAODV RREQ message differs from the one proposed in , it additionally contains the RSA public key of the source node S and is digitally signed to ensure authenticity and integrity of the message. Upon receiving a RREQ message, each node authenticates the source S, by verifying the message integrity and by verifying the signature against the provided public key. Upon successful verification, the node updates its routing table with S's address and the forwarding node's address. If the message is not addressed to it, it rebroadcasts the RREQ.

5.5 BISS

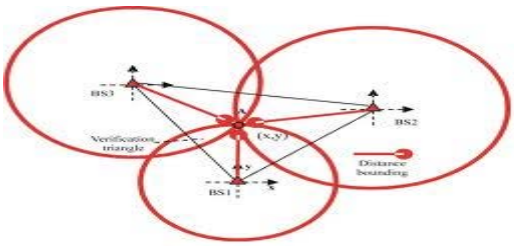

Fig4. Building Secure Routing

Building Secure Routing out of an Incomplete Set of Security Associations (BISS), the sender and the receiver can establish a secure route, even if, earlier to the route detection, only the receiver has security associations recognized with all the nodes on the chosen route. Thus, the receiver will authenticate route nodes unswervingly through security associations. The sender, however, will authenticate directly the nodes on the route with which it has security associations, and indirectly (by exchange of certificates) the node with which it does not have security associations. The operation of BISS ROUTE REQUEST relies on mechanisms similar to direct route authentication protocols.

When an initiator sends a ROUTE REQUEST, it signs the request with its private key and includes its public key *PKI* in the request along with a certificate *cl* signed by the central authority binding its id with *PKI* . This enables each node on the path to authenticate the initiator of the ROUTE REQUEST. The ROUTE REQUEST message contains the id of the target node. The node that receives this ROUTE REQUEST authenticates the initiator (by verifying the signature on the message), and tries to authenticate the target directly through security associations that it has. Only if a node can successfully authenticate both the initiator and the target will the node broadcast the message further. In BISS, we use similar route request data authentication mechanisms as in Adriane.

5.6 SLSP

The Secure Link State Protocol (SLSP) for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within *R* hops, which is termed as their *zone* . Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (*LSU*) packets from malicious alteration, as they propagate across the network.It disallows advertisements of non-existent, fabricated links, stops nodes from masquerading their peers, strengthens the robustness of neighbor discovery, and thwarts deliberate floods of control traffic that exhausts network and node resources. To operate efficiently in the absence of a central key management, SLSP provides for each node to distribute its public key to nodes within its zone. Nodes periodically broadcast their certified key, so that the receiving nodes validate their subsequent link state updates. As the network topology changes, nodes learn the keys of nodes that move into their zone, thus keeping track of a relatively limited number of keys at every instance. SLSP defines a secure neighbor discovery that binds each node *V* to its Medium Access Control (*MAC*) address and its *IP* address, and allows all other nodes within transmission range to identify *V* unambiguously, given that they already have *EV*. Nodes promote the state of their incident links by broadcasting periodically signed link state updates (*LSU*).

SLSP restricts the propagation of the *LSU* packets within the zone of their origin node. Receiving nodes validate the updates, suppress duplicates, and relay previously unseen updates that have not already propagated

R hops. Link state information acquired from validated *LSU* packets is accepted only if both nodes incident on each link advertise the same state of the link.

6. COMPARISONS OF SECURE PROTOCOLS

At the last we provide the comparison of different secure routing protocols of ad hoc network using table 1.Table 2 shows defense against different type of attack. Comparison shows, which protocol, is better in different type of attacks.

Table 2: Protocol defense against different type of attack Table

Attack	Protocol							
	ARAN	SRP	SEAD	ARIADEAN	SAODV	SLSP	OSRP	RAP
Location Disclosure	No	No	No	No	No	No	No	No
Black- Hole	No	No	No	No	No	No	Yes	No
Replay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Worm hole	No	No	No	No	No	No	No	No
Black mail	NA	NA	NA	NA	NA	NA	NA	NA
Denial of services	No	Yes	Yes	Yes	No	Yes	No	No
Routing table poisoning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Rushing attacks	Yes	No	Yes	Yes	No	No	No	Yes

7. CONCLUSION

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing of wireless Ad-hoc networks were discussed. Adhoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The key management protocols are still very expensive and not fail-safe. Numerous protocols for routing in Ad-hoc networks have been proposed. There is a necessitate to make them more secure and strong to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks broad open for research to meet these demanding application.

REFERENCES

[1] Adrian Perrig Ran Canetti J. D. Tygar Dawn Song "*The TESLA Broadcast Authentication Protocol*", UC Berkeley and IBM Research.

[2] Ajay Mahimkar, R. K. Shyamasundar *"S-MECRA A Secure Energy-Efficient Routing Protocol for Wireless Ad Hoc Networks"* IEEE 2004.

[3] Alia Fourati, Khaldoun Al Agha, Hella Kaffel Ben Ayed *"Secure and Fair Auctions over Ad Hoc Networks*" *Int. J. Electronic Business, 2007*

[4] T. Clausen, P. Jacquet, RFC3626 –"*Optimized Link State Routing Protocol (OLSR)"*, 2003.

[5] H. Deng, D.P. Agrawal, *"TIDS: threshold and identity-based security scheme for wireless ad hoc networks*", Ad Hoc Netw. 2 (3) ,2004, pp.291–307.

[6] H. Deng, A. Mukherjee, D.P. Agrawal, "*Threshold and identity-based key management and authentication for wireless ad hoc networks"*, in: Proc. ITCC, IEEE, 2004, pp. 107–111.

[7] S. Goldwasser, S. Micali, R.L. Rivest, *"A digital signature scheme secure against adaptive chosen-message attacks"*, J. SIAM Comput. 17 1158(April) ,1988, 281–308.

[8] F. Hess, "*Efficient identity based signature schemes based on pairings*", in: Proc. SAC: Annual International Workshop on Selected Areas in Cryptography, LNCS, Springer, 2003, pp. 310–324.

[9] A. Khalili, J. Katz, W.A. Arbaugh, *"Toward secure key distribution in truly ad-hoc networks"*, in: Proc. SAINT Workshops, IEEE, 2003, pp. 342–346.

[10]F. Kuhn, R. Wattenhofer, A. Zollinger, "*Asymptotically optimal geometric mobile ad-hoc routing*", in: 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, DIALM'02, 2002.

[11] W. Lee, W. Sriborrirux, *"Optimizing authentication mechanisms using ID-based cryptography in ad hoc wireless mobile networks"*, in: Proc. Information Networking, Networking Technologies for Broadband and Mobile Networks, LNCS, Springer, 2004, pp. 925–934.

[12] Y.-H. Lee, H. Kim, B. Chung, J. Lee, H. Yoon, *"On-demand secure routing protocol for ad hoc network using id based cryptosystem"*, in: Proc. 4th ICPDCAT, IEEE, 2003, pp. 211–215.

[13] G. Li, W. Han, *"A new scheme for key management in ad hoc networks"*, in: Proc. 4th International Conference on Networking Proceedings, LNCS, Springer, 2005, pp. 242–249.

[14] J.V.D. Merwe, D. Dawoud, S. McDonald, *"A survey on peer-to-peer key management for mobile ad hoc networks"*, ACM Comput. Surv. 39 (1) (2007) pp.1–45.

[15] B.-N. Park, W. Lee," *ISMANET: a secure routing protocol using identity-based encryption scheme for mobile ad-hoc networks*", J. IEICE Trans. Commun. (2005) pp.2548–2556.

[16] B.-N. Park, J. Myung, W. Lee, "*ISSRP: a secure routing protocol using identity-based sign encryption scheme in ad-hoc networks*", in: Proc. 5th International Conference on Parallel and Distributed Computing, LNCS, Springer, 2004, pp. 711–714.

[17] B.-N. Park, J. Myung, W. Lee, "*LSRP: a lightweight secure routing protocol with low cost for ad-hoc networks"*, in: Proc. International Conference on Convergence in Broadband and Mobile Networking, LNCS, Springer, 2005, pp. 160–169.

[18] K.G. Paterson, "*ID-Based Signatures from Pairings on Elliptic Curves*". Report 2002/004, Cryptology ePrint Archive, 2002.

[19] C.K. Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Prentice Hall, 2001.

[20] L. Zhou, Z. Haas, "*Securing ad hoc networks*", IEEE Network Magazine 13 (6) (Nov/Dec 1999) pp.24–30.