A Comparative Study for Secure Routing in MANET

Parul Tomar
Dept. of Computer Engineering,
YMCA University of Science and
Technology, Faridabad, India

Prof. P.K. Suri
Dept. of Computer Science and
Application, Kurukshetra University,
Kurukshetra, India

Dr. M. K. Soni
Executive Director & Dean, F.E.T.
MRIU, Faridabad, India

ABSTRACT

In the current era of wireless network, popularity of MANET is increasing at a very fast pace. Reason for this increased attention is the wide range of multimedia applications running in an infrastructure less environment. Because of the infrastructure less environment, limited power and dynamic topology it becomes very difficult to provide a secure environment in MANET. In this paper we are providing a detailed survey of different kind of attacks and proposed solutions for handling those attacks. This paper also gives a brief comparison of various protocols available for secured routing in MANET.

Keywords

MANET, SECURITY, RREP, RREQ, TTL.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication Figure.1. Some special characteristics of MANET like dynamic topology, fast deployment, robustness make this technology an interesting research area. Each node in MANET can work as a sender, receiver as well as router Figure 1. Communication in the network depends upon the trust on each other. Communication can work properly if each node co-operate for data transmission.

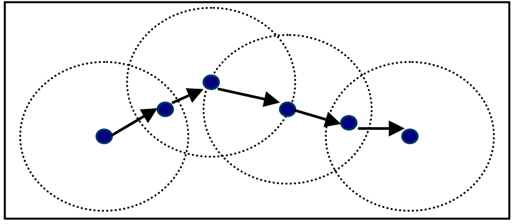

Figure 1. Communication in Mobile Adhoc Network

The following algorithm depicts the communication in any ad hoc network:

1. Sender node sends the signal to the neighboring nodes within the vicinity.
2. Neighboring nodes communicate with the sender node
3. Sender node sends the message to the destination node.
4. If destination node is within the vicinity then message received by the destination node else an intermediate node receives the message.
5. Restart the process of forwarding the message from step no 1 till the destination node is reached.

As MANET has no fixed infrastructure, they are more prone towards the security threats as compared to the infrastructure wireless networks. Providing security in MANET is a difficult task to achieve due to its dynamic nature, lack of centralized monitoring, and limited resources like bandwidth and battery power.

This paper provides a survey on the various security issues, attacks and various proposed routing protocols against these attacks. Paper is divided into three major sections. First section will describe security goals required for secure routing in MANET. Second Section gives detail description of various attacks on MANET. Last section will provide various solutions proposed by the researchers against these attacks.

2. SECURITY GOALS

Every routing protocol needs secure transmission of data. Security service requirements of MANET are similar to wired or any infrastructure wireless network. Following are five major security goals which are needed for protecting the data and resources from attacks:

a) Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.
b) Availability: Availability ensures the survivability of the services even in the presence of the attacks. Availability is concerned with the fact that the network services should be available whenever they are needed. Systems ensuring the availability in MANET's should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehavior.
c) Confidentiality: Confidentiality ensures that information should be accessible only to the intended party. No other node except sender and receiver node can read the information. This can be possible through data encryption techniques.
d) Integrity: Integrity ensures that the transmitted data is not being modified by any other malicious node.
e) Non-Repudiation: Non-repudiation ensures that neither a sender nor a receiver can deny a transmitted message. Non-repudiation helps in detection and isolation of compromised node.

Apart from the above stated issues some other issues need to be taken care of:

I. Cooperation and Fairness

II. Confidentiality of location
III. No Traffic diversion

3. ATTACKS ON MANET [1]

In Infrastructure less networks there is much more need for the security as each node is free to move in any direction and there is no centralized security provision in such networks. Attacks on MANET's are broadly divided into two major categories:

- Active Attacks: Active attacks are those attacks which try to interrupt the proper functionality of the network. This can be done either through reading and changing the information on the data packets, denial of Services, altering the routing path by changing routing information, hop count etc. These attacks are easier to be detected as compare to their counterpart i.e. Passive attacks.
- Passive Attacks: Passive attacks are those attacks which do not alter the normal functionality of network but silently try to listen or retrieve the vital information inside the data packets. These kinds of attacks are hard to detect.

These attacks are further classified into four major categories Figure 2 which are described as follows:

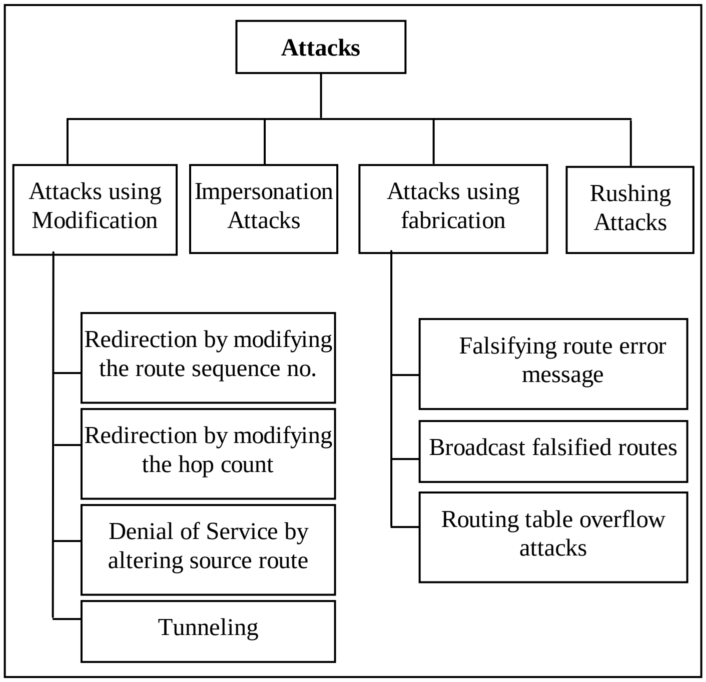
Attacks
Attacks using Modification
Impersonation Attacks
Attacks using fabrication
Rushing Attacks
Redirection by modifying the route sequence no.
Redirection by modifying the hop count
Denial of Service by altering source route
Tunneling
Falsifying route error message
Broadcast falsified routes
Routing table overflow attacks

Figure 2. Various Types of Attacks on MANET

Now let us take each of the attack in detail:

1. Attacks using modification
   a) Redirection by modifying the route sequence number: In order to find the best route to the destination, nodes always depends upon the metric values such as sequence no, hop count, delay etc. Lower the value, best is the path. In this attack malicious node changes the hop count to smaller value than the last smallest value, and can redirect the traffic.
   b) Redirection by modifying the hop count: Here, in this attack packet traffic can be diverted to any compromised node by changing the hop count metrics to a smaller value.
   c) Denial of Service by altering source route: Denial of Service attacks aim at the complete destruction of the routing function. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.
   d) Tunneling: A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.
2. Impersonation attacks: Impersonation attacks are also known as "Spoofing". In this attack, malicious node changes its IP address or MAC address in the outgoing packets and uses the address of another node. Through spoofing any mischievous node can change the network topology or isolate any node from rest of the network.
3. Attacks using fabrication
   a) Falsifying route error message: This type of attack is more prominent in On-demand routing protocol, which uses path maintenance to recover the broken links. Whenever a node changes its location, the closest node sends an error message to the other nodes that this route is no longer exist. By sending this kind of error message any node can be easily isolated.
   b) Broadcast falsified routes: In this kind of attacks attacker exploit the routing information from the packet header and changes the routing path. This will change the route cache of neighboring node.
   c) Routing table overflow attacks: In this kind of attack, the attacker attempts to create routes to non-existing routes. If enough routes have been created, no new routes can be entered in the routing table.
4. Rushing attacks: This kind of attack is applicable on On-Demand Routing protocol. In On-Demand routing protocol only one route request packet is forwarded to find the path to the destination node. This property is being used in Rushing attacks by forwarding the RREQ Packets more frequently than the other nodes so that the route including the attacker will be discovered.

4. SECURE ROUTING FOR MANET

Security protocols for MANET's can be mainly categorized in two major categories:

- **Prevention:** This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information.

- **Detection and Reaction:** Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network.

On the basis of our survey, secure routing protocols can be classified as Figure 3:

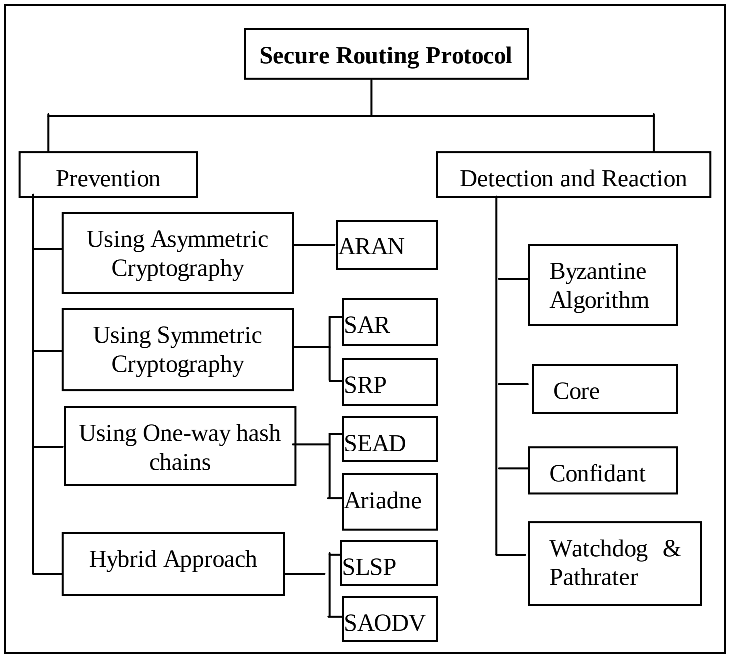

Figure 3. Secure Routing Protocols

Now, let us first take the routing protocols related to prevention schema in detail:

1. *Prevention Using Asymmetric Cryptography*
   a) Authenticated Routing for Ad-hoc Network (ARAN) [2]: Authenticated Routing for Ad-hoc Network (ARAN) is an On-Demand routing protocol which uses the cryptographic certification. This protocol consists of the following steps:
   - preliminary certification step which requires of a trusted certification authority, who distributes its public key to all the nodes in the network. It is necessary for each node to certify its address and to have the public key before connecting to the network.
   - Second step is the route discovery for end-to-end authentication. The goal of end-to-end authentication is for the source to verify that the intended destination was reached. The source begins route instantiation by broadcasting a digitally signed Route Discovery Packet (RDP). The RDP includes the certificate of the initiating node, a nonce, a timestamp and the address of the destination node. Nonce and timestamp are present to prevent replay attacks and to detect looping and appends its signature on the packet. All subsequent intermediate nodes remove the signature of the previous node, verify it and append their signature on the packet. Similarly, along the reply packet (REP) each node appends its signature before forwarding it to the next hop. In order to maintain the route, nodes keep track of whether routes are active or not. An error message is generated and forwarded to the source node if the data is received from an inactive or broken node.
2. *Prevention Using Symmetric Cryptography*
   a) Security Aware Ad-hoc Routing [3]: Security-Aware ad hoc Routing (SAR) makes use of security attributes to take the routing decision. In SAR, security metric is embedded into the RREQ packet. Nodes are required to have keys for decryption of data while forwarding or receiving the data. If a path with the required security attributes is found a RREP is sent from an intermediate node or the destination node to the source node. In case of more than one route the shortest route is selected for data forwarding.

   b) Secure Routing Protocol [4]: Secure Routing Protocol (SRP) is another routing protocol which uses symmetric cryptography. The protocol is based on route querying method. SRP Requires a Security Association (SA) between source and destination node. Key generated by the SA is used to encrypt and decrypt the data by the two nodes.

   A SRP Header (Figure 4) is added to the base header. The RREQ packet consists of a *query sequence number (QSEQ), query identifier (QID)*, and the out put of a key hashed function. The key hash function takes IP header, header of the basic routing protocol, and the shared key.

IP HEADER	
BASIC ROUTING PROTOCOL HEADER	
TYPE	RESERVED
QUERY IDENTIFIER (QID)	
QUERY SEQUENCE (QSEQ)	
MESSAGE AUTHENTICATION CODE(MAC)	

Figure 4. SRP Packet header

   The intermediate nodes broadcast the query to the neighboring nodes and update their routing table. If receiving node has the same QID in their routing table, query is dropped. When the destination is reached, destination node checks for the security metrics by calculating the key hash function "*message authentication code (MAC)"*. After verifying the secret key it generates reply packet for source node consisting of path from source to destination, QID, QSEQ. After receiving the reply packet source node again calculates its MAC. There can be multiple routes from source to destination. Route maintenance in this protocol is also done through route error message.
3. *Prevention Using one-way hash chains*
   a) Secure Efficient Ad-hoc Distance Vector Routing [5]: Secure Efficient Ad-hoc Distance Vector Routing (SEAD) protocol is a proactive routing protocol based on the design of DSDV protocol. This protocol is used against the modification attacks. This protocol makes use of hash chain method for checking the authenticity of the data packet. This hash chain value is used for

transmitting a routing update. A node that receives a routing update, verifies the authentication of each entry of the message. SEAD make use of destination sequence number in order to remove looping.

To avoid loops, SEAD protocol also authenticates the source of routing update message. This can be done with any one of the following two mechanisms: a) make use clock synchronization between the nodes that participate in the ad hoc network, and employs broadcast authentication mechanisms. b) By providing a shared secret Key between pair of nodes for *message authentication code* (MAC) between the nodes for the authentication of a routing update message.

b) Ariadne [6]: Ariadne is an on-demand secure ad-hoc routing protocol based on DSR with symmetric cryptography. This protocol makes use of a shared key between the nodes for authentication (MAC). Ariadne protocol can be carried out in 3 steps which are as follows:

- When source node wants to communicate with other node, it sends a route request (RREQ) containing source address, destination address, an Identifier that identifies the current route discovery, a TESLA time interval denoting the expected arrival time of the request to the destination, a hash chain.
- On receiving the RREQ the intermediate node checks for the validity of the TESLA time interval.
- In order to check the authentication a one-way hash function is used. If data packet is a valid packet then the node appends its own address in the node list, replaces the hash chain with a new one consisting of its address plus the old one, and appends a MAC of the entire packet to the MAC list. The destination node verifies each hop of the path by comparing the received hash and the computed hash of the MAC.

4. *Hybrid approach*

a) Secure Link State Routing Protocol [7]: The Secure Link State Routing Protocol (SLSP) is used to secure the discovery and the distribution of link state information. This protocol makes use of asymmetric key for the security purpose. Participating nodes are identified by the IP addresses of their interfaces.
SLSP can be logically divided into three major steps which are as follows:

- Public key distribution: SLSP do not make use of any central server for key distribution. Distribution of public key is done by the node to the nodes within its own vicinity. This distribution of the key is known as public key distribution (PKD).
- Neighbor discovery: Link state information of the node is broadcast periodically using Neighbor Lookup Protocol (NLP). Hello message contains sender's MAC address and IP address of the network. These messages are also signed. NLP can be used for identifying the discrepancies or the malicious node.
- Link state updates. Link state update (LSU) packets are identified by the IP address of the initiating node and include a 32-bit sequence number for providing updates. Intermediate nodes LSU verify the attached signature using a public key they have previously cached in the pubic key distribution phase of the protocol. The hops_traversed field of the LSU is set to hashed hops_traversed, the TTL is decremented and finally the packet is broadcasted again.
- To protect against denial of service attacks, SLSP nodes maintain a priority ranking of their neighboring nodes based on the rate of control traffic they have observed. High priorities are given to nodes that generate LSU packets with the lowest rate. This functionality enables the neighbors of malicious nodes that flood control packets at very high rates to limit the effectiveness of the attack. .

b) Secure Ad-hoc On-demand Distance Vector Routing Protocol[8]: Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV) is based on AODV routing Protocol. SAODV make use of asymmetric cryptography as well as hash chaining. When a node wants to send a message it digitally signs the RREQ packet (Figure 5) and send it to the neighboring nodes. On receiving a RREQ, intermediate nodes verifies the signature before updating or creating a reverse route to the host with the help of cryptography.

<table>
<tr><td>TYPE</td><td>LENGTH</td><td>HASH FUNCTION</td><td>MAX HOP COUNT</td></tr>
<tr><td colspan="4">TOP HASH</td></tr>
<tr><td colspan="4">SIGNATURE</td></tr>
<tr><td colspan="4">HASH</td></tr>
</table>

Figure .5. SAODV Protocol Header

Hash chains are used in SAODV to authenticate the hop count. When a node wants to send a RREQ or a RREP it generates a random number called as seed. It Selects a Maximum Hop Count which should be set to the TTL value in the IP header. The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Whenever an intermediate node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count - Hop Count times the Hash field and check whether the resultant value is same as Top Hash value. If two values are different from each other, data packet will be dropped by the node. For the broken links an error message is generated by the nodes.

Following are the protocols related to Detection and Reaction schema:

1. Byzantine Algorithm [9]: This protocol is used to protect the network from Byzantine failures which include modification of packets, dropping packets, attacks caused by selfish or malicious nodes.
Byzantine algorithm consists of three different phases (Figure 6):

- Route Discovery: When a source node wants to send the message, it broadcasts a route request packet containing source address, destination address, a sequence number, a weight list and the private key for authentication to its neighbors. On receiving the RREQ packet the intermediate node checks for RREQ entry in its own list. If there is no entry for the RREQ, it verifies the key for authentication and appends it in the list and rebroadcast it to other nodes.

- When the destination node is reached, it verifies the key and creates a route reply message (RREP). On receiving the RREP packet, source node confirms the private key. It also compares the received path and the existing path. If the received path is better than the existing one then update this route in its own table.

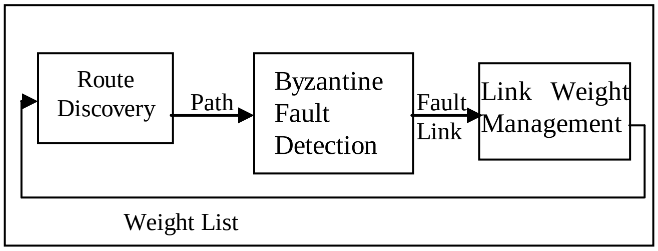

Figure 6. Three phases of Byzantine algorithm

- Fault Detection: In this phase each intermediate node called as probe node sends acknowledgement to source node for every received packet. If number of unacknowledged packets moves above some threshold value, a fault is registered on the path.
- Link Weight Management: This phase of the protocol calculates the weight of the links. If a link is identified as faulty by the fault detection phase its corresponding weight value gets doubled. In the route discovery phase link with lower weight value will be taken as better link.

2. Core [10]: The CORE(a collaborative reputation mechanism to enforce node cooperation in MANET) is a protocol which works on the co-operative behavior of the nodes. It makes use of *Reputation Table* and *Watchdog* mechanism to identify the co-operative or misbehaving node. The *reputation table* component maintains a table of intermediate nodes and the associated reputation or ratings. The Watchdog component calculates the function and provides the Reputation value.
   This protocol consists of a sender and one or more intermediate node. In this protocol, whenever an intermediate node refuses to co-operate with the sender node, CORE scheme will decrease the repudiation of intermediate node. This can lead to elimination of intermediate node from the network.

3. Confidant [11]: The Confidant (Cooperation of Nodes: Fairness In Dynamic Ad hoc NeTworks) protocol is use to identify the non cooperative nodes. This protocol consists of following components: the *monitor*, the *reputation system*, the *path manager* and the *trust manager*.
   The *monitor* component is responsible for monitoring *passive acknowledgements* for each packet it forwards.

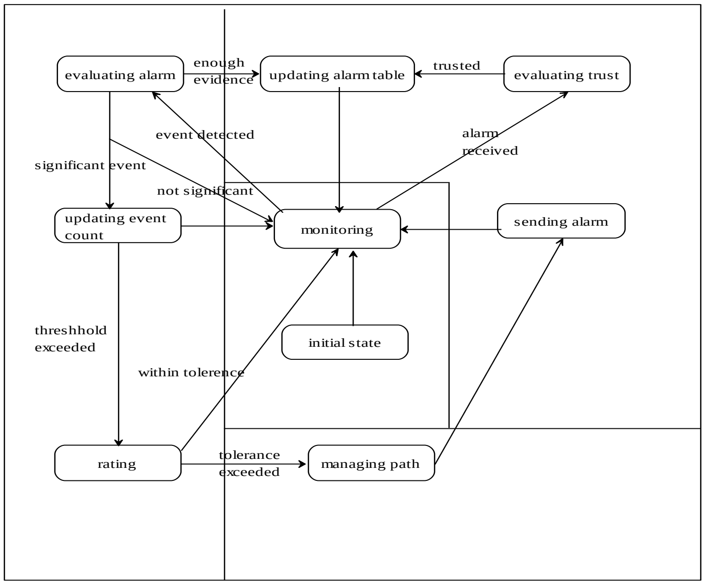

Figure 7. Trust Architecture inside a node

The *trust manager* component deals with the sending and receiving of *alarm* messages [12]. When a node finds that a node is misbehaving, it sends an alarm message. Such messages are exchanged between nodes that are pre-defined as *friends*. Alarms from other nodes are given substantially less weight.

The *reputation system* component maintains a table of nodes and the associated ratings. Ratings are modified according to a *rate function* that makes uses of small weights if an alarm is reported for a misbehaving node and greater weights for direct observations.

The *path manager* component manages all path information regarding addition, deletion, and updating of paths according to the feedback it received from the reputation system. If a rating falls under a certain threshold the path manager component is called in order to remover the path containing the identified malicious node

4. Watchdog and Pathrater[13]: The *watchdog* and *pathrater* protocol is used to find out the malicious nodes which deny forwarding the packets however they have agreed to forward it earlier. The role of *Watchdog* is to watch that the next node in the path is forwarding the data packet or not. If not then it will be taken as the malicious behavior. Role of *pathrater* is to evaluate and find the reliable path from the result generated by watchdog.
   When a node transmits a packet to the next node in the path, it tries to listen if the next node will also transmit it and also tries to find out that the next node do not modify the packet before forwarding it. If a node shows any malicious activity like denial of service or modification of data packet, *Watchdog* will increase its failure rating. This failure rating is helpful in finding out the reliable path from source to destination.

5. COMPARISON OF VARIOUS SECURE ROUTING PROTOCOLS

On the basis of the various studied protocols a comparison table is given below:

Table 1. Comparison Table of Secure Routing Protocols

Proposed protocols	**Routing strategy**	**Security From :**			
		Rushing attack	**Denial-of-service**	**Routing table modific-ation**	**Tunneling**
ARAN	On demand	Yes	No	Yes	No
SAR	On demand	Yes	No	Yes	No
SRP	On demand	Yes	Yes	Yes	No
SEAD	Table driven	Yes	Yes	Yes	No
Ariadne	On demand	Yes	Yes	Yes	No
SLSP	Table driven	Yes	Yes	Yes	No
SAODV	On demand	Yes	No	Yes	No
CORE	Table driven	No	yes	No	No
CONFIDANT	On demand	Yes	No	No	Yes
BYZANTINE	On demand	Yes	Yes	Yes	No
WATCHDOG & PATHRATER	On demand	No	No	No	Yes

Above table displays that a lot of work is done for rushing attacks, Denial –of- service and Table modification attacks but for Tunneling attacks a lot of secure protocols are required. Also, every secure routing protocol can handle only limited attacks. For eg. ARAN and SAR can provide security against rushing and routing table modification attacks, but they are unable to provide security against Denial-of-Service and Tunneling attacks. Similarly, CORE provide security only against Denial-of-Service attacks and Watchdog and Pathrater provide security for Tunneling attacks.

6. CONCLUSION

In this paper, we have presented an overview of the various security goals, security threats and various existing routing protocols supporting security requirements. From the study, a comparison table is provided which clears the fact that all the secure protocol works under various limitation and provide security against limited threats. None of the protocol is able to accomplish all security goals. So, there is still a requirement of more secured protocol that can deal with the various demanding requirements of MANET.

7. REFERENCES

[1] Djamel Djenouri and Lyes Khelladi, Cerist Center Research, Algiers Nadjib Badache, University of Science and Technology, Algiers. A Survey of security issues in mobile Ad Hoc and Sensor Networks.

[2] Kimaya Sanzgiri , Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. A Secure Routing Protocol for Ad Hoc Networks. In 10 Conference on Network Protocols (ICNP), November 2002.

[3] Seung Yi, Prasad Naldurg, Robin Kravets. Security-Aware Ad hoc Routing for Wireless Networks. In Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001.

[4] P. Papadimitratos, Z.J. Haas, P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routing-protocol-00.txt 2002-12-11

[5] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In 4th IEEE Workshop on Mobile Computing Systems & Applications, 2002.

[6] James D.Allen, Patrick T. Gaughan, David E. Schimmel and Sudhakar Yalamanchili. Ariadne- An Adaptive Router for Fault-tolerant Multicomputers. In MobiCom'02, Sep. 2002, pp 23-26.

[7] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[8] Manel Guerrero Zapata , and N. Asokan. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, vol. 3, no. 6, July 2002, pp. 106-107.

[9] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens. An On-Demand Secure Routing Protocol Resilent to Byzantine Failures. WISE'02, Atlanta, Georgia, September 2002, pp. 21-30.

[10] Pietro Michiardi, Refik Molva. Core: A Collaborative REputation mechanism to enforrce node cooperation in Mobile Ad Hoc Networks. In Communication and Multimedia Security Conference, 2002.

[11] Sonja Buchegger, Jean-Yves Le Boudec. Cooperation Of Nodes — Fairness In Dynamic Ad-hoc NeTworks. IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[12] Sonja Buchegger, Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing , EUROMICRO-PDP.02.

[13] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. ACM MobiCom, 2000, pp- 255-265.

[14] Hongmei Deng, Wei Li, and Dharma P. Agrawal. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine, October 2002.

[15] Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic, Routing and Security in Mobile Ad hoc Networks, February 2004.