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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

SECURITY ISSUES AND LINK EXPIRATION IN SECURE ROUTING PROTOCOLS IN MANET: A REVIEW

Parul Singh[1], Gopal Singh[2]

[1]M.Tech, Student, Computer Science, Department of Computer Science & Applications,

Maharshi Dayanand University, Rohtak, Haryana, India[1]

[2]Assistant Professor, Department of Computer Science & Applications, Maharshi Dayanand University,

Rohtak, Haryana, India[2]

Abstract: Link Expiration is a major problem in existing secure as well as non-secure routing protocols of mobile ad hoc network (MANET) and is one of the most encouraging research areas. Due to link expiration packet loss and other routing overhead increased. So, the requirement is both: secure and reliable link. Secure communication in mobile ad hoc networks is difficult due to the following factors: mobility, limited resource availability, dynamic topology and limited processing power. MANETs are highly vulnerable to attacks namely, passive attacks and active attacks. Traditional routing protocols do not provide security. So, various secure routing protocols have been proposed to secure mobile ad hoc network. Link disconnection is another problem in mobile ad hoc network. Due to mobility of nodes link expires and the node has to find another route for sending the data. So, that route must be found in which the link does not expire before all the packets reach the destination. In this paper, the focus is on the security attacks present in the existing secure routing protocols and on those protocols which focus on link expiration time between nodes for sending the packets or data.

Key Words: Security attacks, Protocols, Secure Routing, Malicious nodes, and Link Expiration.

I. INTRODUCTION

Mobile ad hoc network is non infrastructure i.e. it has no base stations or access points, and self-organizing. Due to the mobile nature of devices MANET has no fixed topology and it may change dynamically. So, in MANET, nodes (mobile devices) can move freely and hence the network changes it topology very frequently. Due to the unique characteristics of network, such as dynamically changing network topology, lack of centralized management, mobile nodes etc., and such network is vulnerable to security attacks.

In MANET, routing protocols have been designed to provide reliable routes in the network which are followed by data packets. Depending on the network topology routing protocols can be divided into three types: reactive, proactive and hybrid. These routing protocols are exposed to different types of attacks as packets are forwarded by the nodes present in the network and it is possible that the nodes are malicious. Malicious nodes can disrupt the functioning of routing protocols by modification, fabrication and impersonation. Selfish nodes are also present in the network and their aim is to save battery life for their own communication by not participating in the network operation [1]. The traditional routing protocols do not provide protection against malicious and selfish nodes. The present secure routing protocols provide security during data transmission and to data but for finding the route to the destination these protocols follow the same approach as followed by traditional routing protocols. Many of the traditional routing protocols are based on distance metric; no one is based on time metric i.e., link expiration time. In an active connection, routes are subject to frequent disconnections. In such an environment, it is important to minimize disruptions caused by the changing topology. In order to deliver more packets and utilizing control packets efficiently one may use mobility prediction [28]. Many routing protocols have been proposed which improve their performance by using mobility prediction [28]. These protocols may provide reliable route but security is absent. So there is need for secure and reliable protocols which provide routes which are secure as well as reliable.

This paper provides the comparison of secure routing protocols on the basis of security attacks. The paper is divided into six sections. Section II explains the security attacks present in MANET. Section III explains the security mechanism. Section IV discusses the routing in MANET. Section V explains the mobility prediction in MANET. Section VI discuses the working of protocols based on Predicted Link Expiration Time. Section VII compares and analyses the existing secure routing protocols. Section VIII provides the conclusion.

II. SECURITY ATTACKS ON MANET

There is a wireless link between nodes in ad hoc network. These links are susceptible to attacks like eavesdropping, interception, impersonation, denial of service and modification. Attacks can be divided into:-

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

External attacks: A node which is not allowed to access the network launches the attacks. The aim is to cause congestion, and propagate wrong routing information.
Internal attacks: Internal compromised nodes launch this type of attack. Wrong routing information is broadcasted to other nodes within the network. It is difficult to detect such wrong routing information because compromised nodes are capable of generating valid signatures using their private keys. [2]
Passive attacks: Collection of information is a passive attack i.e. the attackers aim is to obtain information in transit. This attack does not disrupt the operation of the network. This means that the attacker eavesdrops the packets and attempts to discover valuable information. Passive attacks are harder to detect. This attack includes release of message contents and traffic analysis. Here, the security requirement confidentiality is violated.
Active attacks: Active attacks are those in which the contents of the message are modified in some manner. This attack disrupts the normal functioning of the network. The active attack is performed with the aim of damaging other nodes. The attacker is able to inject fake or wrong packets into the network to perform this attack. So, active attacks can be in the form of interruption, modification and fabrication. There are different types of active attacks possible in mobile ad hoc network. Some of them are discussed below:

- *Blackhole attack:* This attack is the network layer attack. It has two properties [3]. The malicious node falsely advertises of having a valid and shortest route to the destination so that it can intercept the packets and legitimate nodes route data packets through this malicious node. The malicious node does not forward the packet and drops it.
- *Wormhole attack:* It is also a network layer attack. In this attack, packets are received by the attacker at one location and tunnel them to another location in the network. This tunnel between two colluding attackers is referred as a wormhole [3]. Routing can be disrupted when routing control messages are tunnelled. In this attack, wormhole nodes are connected through a tunnel that creates the illusion that the two regions are directly connected, making believe that they are neighbors but in reality they are not. The apparent neighbors are connected through a secret communication channel or tunnel to create this shortcut, which is generated by an attacker that introduces transceivers connected to each other with a high quality, low latency link. In this way, the attacker takes the transmitted packets in one region and reinserts them into another region [4].
- *Spoofing attack:* This attack is also called impersonation attack. In this attack, malicious node represents its identity incorrect by altering its MAC or IP address i.e. the attacker pretends to be another entity. As the attacker poses as a good node it can alter the network topology. Example of this attack is forming loops.
- *Rushing attack:* It is a network layer attack. In on-demand routing protocols, during route discovery process each node receives the Route_Request packet and also the malicious node present in the network receives it. The nodes discard the duplicate packets that arrive later. Now the malicious node floods the packet quickly [5] that it has received, before other nodes can react. So, when the good nodes forward the packets, these packets have been discarded by nodes as they have already received the packets from malicious node. Now, the route from the source node to the destination also contains the malicious node as the intermediate node. So, this route is not secure because it contains malicious node. Rushing attack is very difficult to detect.
- *Denial of Service (DOS) Attack:* DOS attacks are those attacks in which it makes an attempt to prevent legitimate nodes from accessing services or resources. The malicious node floods the network and denies other nodes from using network services. This attack could be launched from any layer. So, in this attack malicious node floods irrelevant data to consume network bandwidth or to consume the resources of a particular node.
- *Byzantine attack:* It is a network layer attack. In this attack compromised nodes work alone or in collusion, carries out attacks such as routing loops creation, forwarding packets on non-optimal paths, and dropping packets. This results in disruption or degradation of the routing services [3]. This attack is hard to detect.
- *Repudiation attack:* An application layer attack in which a node refuses that it has participated in the communication. Here, the security requirement non repudiation is violated.
- *Routing Table Overflow attack:* A network layer attack. Here, the malicious node advertises routes about those nodes which do not exist in the network to the legitimate nodes so that the legitimate nodes do not create entries in its routing table corresponding to new routes to authorized nodes. Here, the aim is to cause an overflow of routing table.
- *Replay attack:* In this attack old routing packets (containing stale routes) are forwarded by the attackers to the legitimate nodes. Other nodes store this stale route in their routing table believing that it is a new route. This attack can disrupt the routing operation [6].
- *Colluding Misrelay attack:* This attack is performed to disrupt the normal routing functioning. In this attack, two or more attackers work in collusion. An attacker near to the source node forwards the packet to another attacker as usual but another attacker can do anything with this packet i.e. modifies or drops it [6].

There are various kinds of attacks possible in mobile ad hoc network. Due to Manet's unique characteristics they are highly vulnerable to attacks. It is a challenge to provide security to these networks. The existing routing protocols allow exploits like modification, impersonation and fabrication against them. So, to secure the communication between nodes secure routing protocols are required. Many secure routing protocols have been proposed to provide secure communications such as ARIADNE [22], ARAN [23], SEAD [24], SAODV [25], SRP [26] etc.

III. SECURITY MECHANISM

Security mechanism is used to provide and enforce security requirements. The secure communication between

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

the source and destination can be achieved through authentication of messages, confidentiality and integrity preventing disclosure and modification of messages. So, establishment of security association between source and destination is required. The technique, cryptography, is used to achieve the security. The existing secure routing protocols use cryptographic mechanism to provide security.

- *Cryptography:* It is the art of achieving security by transforming plain text into cipher text i.e. a message that is not readable by anyone except the intended receiver. Security requirements are the main goals of cryptography. The process of encryption and decryption is used in cryptography. Keys, a small amount of information, are used for performing encryption and decryption. There are two cryptographic algorithms- symmetric key algorithm and asymmetric key algorithm.

Symmetric Key Cryptography: In this scheme, same key (also called secret key) is used for encryption and decryption of messages by sender and receiver respectively. Here, the sender and the receiver must agree upon the key before any transmission starts. This cryptography is also known as Private Key Cryptography. There are number of symmetric key algorithms: DES, IDEA, AES, etc.

Asymmetric Key Cryptography: In this scheme, a pair of key is used i.e. public key and private key. One key is used for encryption and the other must be used for decryption. Public key is known to all the parties but private key is kept secret. If the sender wants to send the message, it encrypts the message with the receiver's public key and sends the message then the receiver decrypts the message with its private key. So each communicating party needs a pair of key (public key and private key). This cryptography is also termed as Public Key Cryptography. Example of asymmetric key algorithms is RSA, ECC, etc.

- *Hash Function:* The problems associated with asymmetric key cryptography are slow operation and large size of encrypted message. So, message digest (hash) can be used to verify the integrity of the message. Hash function is applied over the message to produce its hash. The message along with the hash is sent. The receiver then compares its hash values with those received from the sender. If the values match then receiver will know that message is not modified by anyone in transit. Example- MD5.

IV. ROUTING IN MANETS

Routing Protocols have been designed to find the path from a source node to target node and the data packets travel this path so that it could reach to destination. Routing protocols should have these characteristics: minimal overhead, minimal processing overhead, discover multihop routes, avoiding loop creation, and dynamic topology maintenance [7]. Various routing protocols have been proposed for MANET. Routing protocols in MANET can be classified as:

- Proactive (Table Driven) Routing Protocols
- Reactive (On-Demand) Routing Protocols
- Hybrid Routing Protocols

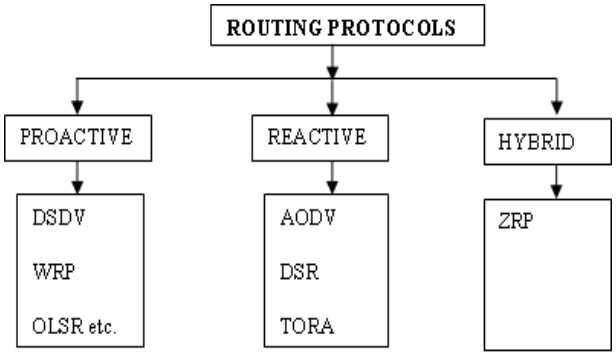

Fig. 1. Classification of routing protocols in MANET

A. *Proactive Routing Protocols*

These protocols maintain a route from each node to every other node at all the times in the network. Each node maintains one or more routing table to store routing information. Tables are updated frequently so that it has consistent and correct routing information. Updates are periodic and event-triggered. In periodic updates routing information is exchanged at specific intervals, on the other hand, event triggered updates are sent when some event occurs [7]. When the network is large, normal communication involves delay in route setup. In this routing, when a node enters or leaves a network, it has to tell its neighbor nodes about its presence. All the nodes need to find the best route to the node and vice versa [2]. Some of the proactive routing protocols are DSDV [8], WRP [9], OLSR [10].

B. *Reactive Routing Protocols*

These routing protocols do not exchange routing information periodically. Information is exchanged or updated only when a path is needed by the source node. Here routes are created on demand i.e. when a node wants to send packets to the destination, then it initiates a route discovery for finding the path to the destination by broadcasting the route request packet if the route does not exist in the source node table. So, there is no need of maintaining routes to each and every node in the network. In these protocols when a node either leaves or enters the network, it does not have to make its presence known to other nodes. Some of the reactive routing protocols are AODV [11], DSR [12], TORA [13].

C. *Hybrid Routing Protocols*

In hybrid routing protocols the features of both proactive and reactive routing protocols is combined. The protocols use both proactive and reactive approach under different sets of conditions. ZRP [14] is a hybrid routing protocol.

These routing protocols are not secure. They are vulnerable to various kinds of attacks. So, these existing routing protocols do not provide security against various kinds of attacks such as [16]:

-Attacks Using Modification: modification of sequence number, hop counts and source routes, tunneling.

-Attacks Using Impersonation: loop formation by spoofing.

-Attacks Using Fabrication: fabrication of error messages and source routes.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

These routing protocols sometimes does not provide the reliable route i.e. the route they have chosen for sending the packets may not be reliable. Consider if any link breaks then the protocol has to initiate the route maintenance activity which increases overhead. Link disconnection also leads to loss of packets. So, those protocols are required which choose that route which stay connected for longer time. Some of the routing protocols are discussed in section 5 which uses mobility prediction [28] for finding the route. Security is also required in mobile ad hoc networks. Many secure routing protocols have been proposed which provide protection against many security attacks.

V. MOBILITY PREDICTION IN MANET

More data packets are delivered to the destinations and control packets are utilized efficiently with mobility prediction. By using mobility prediction, reliable routes are found and all the links of the route stay connected for longer time. The mobility prediction method is predicting Link Expiration Time (LET), in which GPS provide the location and mobility information.

A. Link Expiration Time (LET)

In [28] a mobility prediction method has been introduced which utilizes location and mobility information provided by GPS. Given the motion parameters of two neighboring nodes, the duration of time the two nodes will remain connected can be predicted as follows: Assume two nodes m and n be within the transmission range of each other. Let (x_m, y_m) and (x_n, y_n) be the coordinates of mobile nodes m and n respectively. Let v_m and v_n be the velocities, Θ_m and Θ_n be the direction of motion of nodes m and n, respectively, where $\Theta_m \geq 0$ and $\Theta_n \leq 2\pi$. Then, the amount of time the two nodes m and n will stay connected, LET_{m-n}, is predicted by the following formula: [28]

$$LET_{m-n} = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)^2}}{a^2+c^2}$$

Where, $a = v_m cos\Theta_m - v_n cos\Theta_n$, $b = x_m - x_n$, $c = v_m sin\Theta_m - v_n sin\Theta_n$, $d = y_m - y_n$

VI. ROUTING PROTOCOLS BASED ON PREDICTED LINK EXPIRATION TIME

Routing Protocols have been designed to find the path from a source node to target node and the data packets travel this path so that it could reach to destination. The traditional routing protocols studied above find the route on the basis of distance metric. The protocols discussed below uses mobility prediction method [28] for routing the traffic. Some of them are:

- *Flow Oriented Routing Protocol (FORP):* An on demand Flow Oriented Routing Protocol (FORP) [17] routes real time traffic in MANET using mobility prediction. In this protocol, the sender sends the flow to the destination by constructing a route to it on demand. If the source node has an expired route in its routing table, it broadcasts FLOW-REQ message to find the route to the destination. The node forwarding the message appends its own id and LET. At the destination RET is determined for the route by using the minimum of the set of LETs. A FLOW-SETUP message is sent back to the source node by destination node if the received route is more stable than the one currently in use. On receiving the message the intermediate nodes set up the flow state. The destination node generates the FLOW-HANDOFF message when the route is about to expire. When the source node receives the message, it determines the best route based on the information contained in the message. Then the source node sends the FLOW-SETUP message along the new route.
- *On-Demand Multicast Routing Protocol (ODMRP):* Mobility prediction method is also applied on On-Demand Multicast Routing Protocol [18]. In this protocol, the source node establishes and updates the multicast routes and group membership on demand. The source node periodically broadcasts the JOIN DATA packet to the entire network. When the multicast receiver receives this packet it creates and broadcasts the JOIN TABLE to its neighbors. During this process, routes are constructed from sources to receivers. When the source sends JOIN-DATA packet, it appends its location, speed and direction. The next hop then predicts the link expiration time (LET) between itself and the previous hop. The minimum (between this value and MIN_LET) is included in the packet. The minimum between the last link expiration time and the MIN_LET value is the Route Expiration Time (RET). This value of RET is enclosed in the JOIN TABLE and broadcasted. When the source node receive many JOIN TABLE, it selects the minimum RET among all the JOIN TABLE. Then the source can build new routes by flooding the JOIN DATA.
- *LET-CDS:* The LET based CDS (Connected Dominating Sets) algorithm [19] builds the CDS based on edge weights. Here the edge weights are the predicted link expiration time. The edge having the largest predicted LET is included into the CDS Edge List and the constituent nodes of the edge become part of CDS Node List. The neighbors and the incident edges are also said to be covered. If an edge has higher link expiration time and is the next candidate edge to be considered for inclusion into the CDS, this edge is added to the CDS Edge List if either of its end nodes of the edge has at least one neighbor node that is yet to be covered. This procedure is repeated until all the nodes are covered.
- *Quality of Service (QoS) aware Multicast Routing Protocol with Mobility Prediction (MPQMRP):* In QoS aware Multicast Routing Protocol with Mobility Prediction (MPQMRP) [20] the source node initiates the route discovery by broadcasting the route request packet to its neighbors. The node looks in its routing table for the destination when it receives the route request packet. The node checks the available bandwidth between them if it does not match. The node will use the location information for finding the LET between the nodes and for this the available bandwidth must be above the constrained bandwidth. After updating the information, the intermediate nodes then forward the route request packet to their neighbor nodes. Each node receiving the route request packet calculates the LET between the nodes. The destination node sends the route reply packet. On receiving the route reply packets the source node selects

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

the path having maximum RET. This protocol also includes route maintenance process.

- *Speed Aware Routing Protocol (SARP):* Speed Aware Routing Protocol [21] algorithm is based on demand-supply optimization approach. During the route discovery phase, when the neighbor node receives route request packet from the source node, it determines whether the packet sending node is too fast to form a reliable route. If it is too fast, the neighboring node rejects the packet sending node as a potential one-hop link. The packet sending node is too fast to form a reliable route is determined by calculating the LET. This LET (supply LET) is measured against the predetermined value (LET demanded by the network) for the determination of route reliability. Here, the LET is calculated with respect to the packet sending node. When the value of supply LET is lower than that of addition of demanded LET and time lenience factor, the link is predicted to be ineffective for the required amount of time; and hence the packet is dropped and the sending node is excluded from route inclusion.

A. Analysis

All these above discussed routing protocols based on link expiration time focuses on the reliable routes but security of data or secure route has not been discussed in these routing protocols. So, these protocols proposed to reduce control overhead and send more packets on the route (loss of packets may be less), and nodes stay connected for longer time. But when security is concerned, these protocols do not prevent it from various security attacks. Malicious nodes or compromised nodes might be present in the route chosen by the protocols. So, there is need for both secure and stable routes in MANET.

VII. ANALYSIS OF SECURITY IN SECURE ROUTING PROTOCOLS

MANET relies on the cooperation of all the participating nodes. All the secure routing protocols detect manipulations of data but selfish nodes have not taken into account by them. Selfish nodes are those that do not forward packets and drops them. These nodes deny packet forwarding because they want to save their own resources and use the services and resources of others. So, they degrade the performance of network and partition the network [1]. In this section, analysis of security in secure routing protocols is discussed.

- *ARIADNE:* In ARIADNE [22] authenticity is provided which ensures that request came from the legitimate node not from any malicious node. The initiator can authenticate each entry of the path in the ROUTE REPLY packet as each intermediate node appends a Message Authentication Code with its TESLA key. No intermediate node can remove a previous node in the node list in the REQUEST or REPLY packet using one-way hash function [22]. So, in ARIADNE, modification in the node list of REQUEST or REPLY packet can be detected. Hence, ARIADNE copes with attacks using modification and fabrication of routing information and impersonation by malicious nodes. All routing traffic sent by legitimate nodes which is within range of passive attackers can eavesdrop on it. Traffic can also be analyzed if any packets forwarded by nodes are within range of the attackers. It is not immune to wormhole attack in this version. In its advanced version it uses TIK protocol so it is immune to wormhole attack. No cache poisoning attack is present as ARIADNE protects from flood of ROUTE REQUEST packets.
- *ARAN:* ARAN [23] introduces authentication, message integrity and non-repudiation as a part of minimal security to the MANET environment [23]. End-to-end authentication and routing messages' authentication at each hop from source to destination and vice versa are guaranteed by ARAN. ARAN will not be secure if the trusted authority gets compromised. No spoofing attack is possible in ARAN because source and destination node signs the packet so nodes cannot be spoofed. Those nodes that have certificates, they may fabricate routing messages then ARAN does not prevent fabrication. So, it provides a solution that the node which is injecting false messages continuously may not be taken in future path computation. Authenticated nodes may send unnecessary route requests, so effective DOS attacks are present in ARAN [27]. Wormhole attack is present in the ARAN.
- *SEAD:* SEAD [24] is robust against multiple uncoordinated attackers or active attackers or compromised nodes which create wrong routing state in other node. This protocol is designed to overcome attacks such as DOS attacks and resource consumption attacks [15] [24]. SEAD authenticates sequence number and metric but it cannot prevent malicious node from using same metric and sequence number. If an attacker compromised the nodes then it can successfully send routing messages. SEAD is not immune to wormhole attack.
- *SAODV:* SAODV [25] prevents impersonation of source and destination nodes and forging of error messages. So, only end nodes are authenticated. It prevents malicious node from modifying mutable fields of packet. Nevertheless increasing the hop count by an arbitrary number and thus rejecting unwanted traffic is still possible. Malicious node can forward the received authenticator and hop count without changing them. It is immune to blackhole attack by disabling the intermediate nodes to send reply. If reply is send by the intermediate node then the correctness of the route is checked by sending the enquiry. Wormhole attack is present in SAODV.
- *SRP:* SRP [26] fight against attacks that disrupt the route discovery process and guarantees that the route discovered is correct. Intermediate nodes are not authenticated. SRP copes with non-colluding malicious nodes that are able to modify, replay and fabricate routing information. Source node detects and discards bogus replies. SRP suffers from route cache poisoning attack in its basic version as invalid information is collected in promiscuous mode because it is fabricated by malicious nodes. Route error packets are not verified in SRP [1].

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

TABLE I
COMPARISON OF SECURE ROUTING PROTOCOLS

Protocols	**Routing Approach**	**Routing Protocols**	**Security Mechanism**
ARIADNE	Reactive	Based on DSR	Symmetric key Cryptography, One-way Hash Function
ARAN	Reactive	Based on AODV, DSR	Asymmetric key Cryptography
SEAD	Proactive	Based on DSDV	One-Way Hash Function
SAODV	Reactive	Based on AODV	Asymmetric key Cryptography, One-Way Hash Function
SRP	Reactive	Extension; compatible with DSR, IERP of ZRP.	Security association between source and destination (negotiated shared secret key)

TABLE II
PROTECTION AGAINST ATTACKS

Protocols	**Attacks**				
	Wormhole Attack	**Spoofing Attack**	**Blackhole Attack**	**Dos Attack**	**Rushing Attack**
ARIADNE	Yes	Yes	Yes	Yes	No
ARAN	No	Yes	Yes	No	No
SEAD	No	No	No	Yes	Yes
SAODV	No	Yes	Yes	No	No
SRP	No	Yes	No	Yes	No

Those routes could be harmed by the malicious nodes on which it is present. If the route has more than one attacker then routing loops could be created. [26]

The Table I compares the secure routing protocols and Table II shows secure routing protocols' protection against attacks.

All these secure routing proposals provide secure transmission of data and protection against various attacks. But, the way of discovering route is same as that of traditional routing protocols. In an active connection, routes are subject to frequent disconnections. Due to the high mobility of nodes, the network topology of MANETs changes very fast, making it more difficult to find the routes that packets use. In such an environment, it is important to minimize disruptions caused by the changing topology. Many routing protocols discussed in section 5 have been proposed which improve their performance by using mobility prediction method [28] but these protocols do not provide protection from various security attacks.

VIII. CONCLUSIONS

This paper analyzed the security attacks and link expiration in the routing protocols. The existing non-secure routing protocols do not provide security as well as sometimes link reliability.

Currently, many secure routing protocols have been proposed to provide defense against security attacks. They have taken into account various active attacks performed by malicious nodes but still there are some challenges that are not addressed such as passive attacks and selfishness problem. So, there is not any secure routing protocol that addresses all the security problems present in MANET.

The present secure routing protocols route discovery process is somewhat same as the traditional routing protocols. So, the route on which packets travel might not be reliable. Due to the high mobility of nodes, the network topology of MANETs changes very fast, making it more difficult to find the routes that packets use. In such an environment, it is important to reduce disruptions caused by the changing topology. In this paper few routing protocols which are based on predicted link expiration time are also discussed but these protocols do not provide security. So, protocols which provide connectivity of mobile nodes till message reaches the destination and protection against various security attacks need to be proposed.

REFERENCES

[1] Refik Molva and Pietro Michiardi, "Security in Ad hoc Networks", Personal Wireless Communications, 2003 – Springer.

[2] L. Ertaul, D. Ibrahim, "Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)", Security and Management, 2009.

[3] BingWu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - –c° 2006 Springer.

[4] Felipe Téllez and Jorge Ortiz, "Behavior of Elliptic Curve Cryptosystems for the Wormhole Intrusion in MANET: A Survey and Analysis", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.9, September 2011.

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson," Rushing Attacks and Defense in Wireless Ad Hoc Network", Proceedings of the ACM Workshop on Wireless Security 2003, September 2003.
[6] B. Kannahavong, H. Nakayama, Y. Nemoto, N. Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE Wireless Communication, October 2007.
[7] S. Basagani, M. Giordano, I. Stojmenovic, "Mobile Ad Hoc Networking", John Wiley & Sons, 2004.
[8] Perkins, Charles E., and Pravin Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers", ACM SIGCOMM Computer Communication Review, Vol. 24, No. 4, ACM, 1994.
[9] Murthy, Shree, and Jose Joaquin Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks", Mobile Networks and Applications 1.2 (1996): 183-197.
[10] Jacquet, Philippe, et al., "Optimized link state routing protocol for ad hoc networks", Multi Topic Conference, 2001, IEEE INMIC 2001, Technology for the 21st Century, Proceedings IEEE International, IEEE, 2001.
[11] C. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.
[12] Johnson, David B., and David A. Maltz, "Dynamic source routing in ad hoc wireless networks", Mobile computing, Springer US, 1996, 153-181.
[13] Park, Vincent D., and M. Scott Corson, "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing", Computers and Communications, 1998, ISCC'98, Proceedings Third IEEE Symposium on, IEEE, 1998.
[14] Haas, Zygmunt J., "A new routing protocol for the reconfigurable wireless networks", Universal Personal Communications Record, 1997, Conference Record., 1997 IEEE 6th International Conference on, Vol. 2, IEEE, 1997.
[15] C. Siva Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks", Pearson Education, 2004.
[16] Djamel Djenouri, Nadjib Badache, "A Survey on Security Issues in Mobile Ad hoc Networks", IEEE communications surveys, 2005
[17] Su, William, and Mario Gerla, "IPv6 flow handoff in ad hoc wireless networks using mobility prediction", In Global Telecommunications Conference, 1999, GLOBECOM'99, vol. 1, pp. 271-275, IEEE, 1999.
[18] Lee, Sung-Ju, William Su, and Mario Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks", Mobile Networks and Applications 7.6 (2002): 441-453.
[19] P. Fly, N. Meghanathan, "Predicted Link Expiration Time Based Connected Dominating Sets for Mobile Ad Hoc Networks", IJCSE, Vol. 2 No. 6, 2010.
[20] G. Santhi, Dr. A. Nachiappan, "Adaptive QoS Multicast Routing with Mobility prediction in MANETS", IJASUC, Vol. 1, No. 3, 2010.
[21] Kirthana Akunuri, Ritesh Arora, Ivan G. Guardiola, "A Study of Speed Aware Routing for Mobile Ad Hoc Networks", International Journal of Interdisciplinary Telecommunications and Networking, Volume 3, Issue 3, July 2011, pages 40-61.
[22] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing for Ad Hoc Networks", Wireless Networks 11, 21–38, 2005 Springer Science + Business Media.
[23] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of IEEE ICNP 2002, November 2002.
[24] Yih-Chun Hu, David B. Johnson, Adrian Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Published by Elsevier B.V., 2003.
[25] Z. Manle Guerrero, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", August 2001. http://www.cs.ucsb.edu/~ebelding/txt/saodv.txt
[26] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[27] A. Mahmoud , A. Sameh, S. El-Kassas, "Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)", IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.
[28] W. Su, S.-J. Lee, M. Gerla, "Mobility Prediction and Routing in Ad Hoc Wireless Networks", Int'l J. Network Management, vol. 11, no. 1, pp. 3-30, Feb. 2001.