Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Mobile ADHOC Network and Security Attacks on Network Layer

Martin K Parmar*
Computer Science & Engineering
L.D College of Engineering, Ahmedabad
Gujarat Technological University, India

Harikrishna B Jethva
Associate Prof. of Compute Engineering
L.D College of Engineering, Ahmedabad
Gujarat Technological University, India

***Abstract*— Mobile Adhoc network is gaining popularity today because of their mobility support through which any node can move to any where as long as in the range of radio signal. Topological network is fully dynamic where any node can easily added into network. Every node sends packet to his neighbors' node for those routing protocols provides efficient rout discovery. But bad factor about mobile Adhoc network is that the security often violated. There are number of key issues like limited bandwidth, memory and battery power, no administrator and weak security policy. Because of this nature MANET is more vulnerable than wired network. The use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. This paper mainly focused on the most potential network layer attacks which seriously degrade the performance of the network.**

***Keywords*— MANET, Routing, Security Attack, Network Layer, Mobility**

I. Introduction

Mobile Adhoc network has completely dynamic environment in which any number of nodes can join or leave the network. Entire network are interconnected using wireless link. There is no any centralized administrator as wired network so any node acts like a router to forward packet to its neighbor's node. Entire network is infrastructure less so mobile adhoc network is cheaper than wired network. Because of infrastructure less characteristics the adhoc network can easily setup from anywhere with less efforts and in quick time. Moreover any node can easily add or remove from network without any overhead or disturb other operation. Routing protocol also helps to route packet smoothly and provide better route discovery and route maintenance in case of link failure. Due to the dynamic nature in topology, mobility and decentralized approach there are much chance for attackers to perform malicious activities such like packet capturing, packet dropping, and creating false rout, getting the information of entire topology or structure of network.

MANET Characteristics

- ➢ Open medium.
- ➢ Decentralized.
- ➢ Dynamic topology.
- ➢ Infrastructure less.
- ➢ Distributed cooperation.

MANET Challenges

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that add to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.
- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate), interference, and frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and unidirectional links.
- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks.
- Frequent network partitions- The random movement of nodes often leads to partition of the network. This mostly affects the intermediate nodes.

The key challenges which are faced at different layers in MANET are show in figure in layered structure.

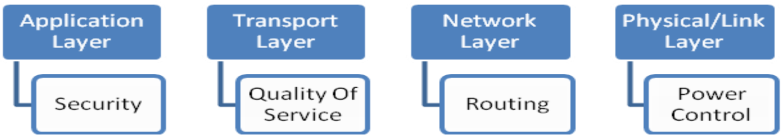

Fig. 1 Key challenges on different layers [1]

II. MANET ROUTING

Routing is process of transferring the packets between the networks or among the networks from one host node to the opposite. Based on the network structure, routing is classified as flat routing, hierarchical routing and geographic position routing. Proactive (table-driven) and reactive (on demand) protocols comes below flat routing, wherever in table driven routing every node keeps the knowledge regarding routing of all alternative nodes within the network and updating of routing information is done once the topology changes. The routing details are kept on routing table at every node. The reactive protocol establishes route only when needed and support route requests and replies between the nodes. Hybrid protocols area unit meant for merging the positive and negative aspects of proactive and reactive protocols.
Characteristics of Proactive, Reactive and Hybrid protocols are shown in table.

Table I
Comparison of Proactive, Reactive and Hybrid [2]

Characteristics	**Table Driven(Proactive)**	**On Demand(Reactive)**	**Hybrid**
Network Structure	Flat	Flat	Hierarchical
Periodic updates	Required	Using Route Discovery	Both
Routing Overhead	Yes	No	Medium
Maintain Route	Always	When needed	Both
Delay for route determination	Little or no	Significant	Medium
Consume bandwidth	More	Less	Less
Network View	Global	Partial	Both
convergence	Slow	Quick	Medium
Scalability	Low when network grow	High	Very High
Example	DSDV,LSR,OLSR, GeoGRID,ALARM.	AODV,DSR,SAR, SPAAR,PRISM	ZRP

Based on literature survey of various Routing Protocols, the Comparison among various protocols under category of Proactive, Reactive and hybrid are shown in table.

Table II: Comparison of Routing Protocols [3], [4]

Protocol	**Location/Identity Centric**	**Advantage**	**Disadvantage**	**Security/ Privacy**	**Encryption Method used(if any)**
LSR	Identity based	Fast, loop free convergence and complete view of network topology.	Demand more memory, more cpu processing and costly on propagating information.	No	No
DSDV	Identity based	Quick reaction when topology changes.	Unnecessary overhead of unused routing information.	No	No
AODV	Identity based	Reduce overhead of control message.	Performance degrades in high traffic.	No	No
DSR	Identity based	Reduce message overhead and faster route discovery.	Lack of security.	No	No
OLSR	Location based	Reduce flooding overhead and reduce the size of control packet.	Consume more resource than AODV. No security and privacy.	No	No
GeoGRID	Location based	Reduce network traffic and give optimal performance in crowed.	No any parameter defined for security measurement.	No	No
SAR	Identity based	Routing do only through trusted nodes.	Not cope with security required in high risk environment.	Yes	Symmetric encryption

SPAAR	Location based	Reduce routing overhead and provide security.	Produces processing overhead using asymmetric cryptography.	Yes	Third party certificate
PRISM	Location based	Exposes only small part of topology and provide security and privacy.	Limits on availability of routes.	Yes	Group Signature
ALARM	Location based	Provides protection against insider and outsider attackers.	Doesn’t scale well in large network.	Yes	Group Signature

III. Security Issues

Security could be a dominant concern in mobile ad hoc network (MANET) as a result of its intrinsic vulnerabilities. These vulnerabilities are nature of MANET structure that can't be removed. As a result, attacks with malicious intent are and can be devised to use these vulnerabilities and to cripple MANET operations. Mobile ad-hoc network is extremely receptive to security attacks because of its open medium, dynamically changing network topology; cooperative algorithms, lack of centralized monitoring and management point, and lack of a transparent line of defense. These vulnerabilities are nature of MANET structure that can't be removed. As a result, attacks with malicious intent are and can be devised to use these vulnerabilities and to cripple MANET operations. There are two types of attacks found in MANET.

A. *Passive Attack*

Passive attacks do not disrupt the normal operation of network. Passive attacks only snoop the data which is exchanged in network. They also capture information about structure of network and types of topology. Passive attack doesn’t alter or modify package but perform eavesdropping, traffic analysis and monitoring.

B. *Active Attack*

Active attacks perform malicious activities which are modification of packet, altering content of data, misrouting, false rout discovery. They also drop the packet. Active attacks are fall into two categories which is internal and external attack.

1) *Internal Attack:*

Internal attack act as valid node and perform malicious tasks. They can access the communication link and advertise false routing. Internal attacks are very hard to detect as they look like a normal node.

2) *External Attack:*

External attack are not a part of network but they are from some another entity or network. External attacks are often mere steppingstones leading to internal attacks, when an outside attacker gains total control of network node.

IV. Potential Attack ON Network layer

There are some attacks as shown in fig. 2 which are much harder to detect and to prevent on network layer and they seriously degrade the network performance.

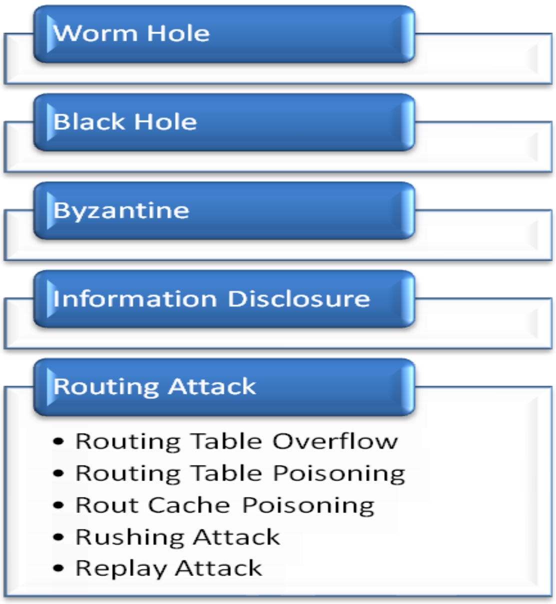

Fig. 2 Attacks on Network Layer [5]

A. *Wormhole Attack*

Wormhole attack at network layer is the most attention seeking attack in ad hoc network. In wormhole attack, two colluding nodes are involved and one node tunnels the packet to another node in the same network over a high speed private wired link or wireless link. These packets are then resent from that location into the network. This tunnel between two malicious nodes is known as wormhole. This attack can easily be launched against communications that resort to authenticity and confidentiality. For example, consider an attack against AODV in Fig. 3, an ad-hoc on demand reactive protocol, in which W1 and W2 are two colluding attackers. Packet is routed from source node N1 to destination node N6.Here malicious node W1 capture the packet and tunnel to another end of malicious node W2.

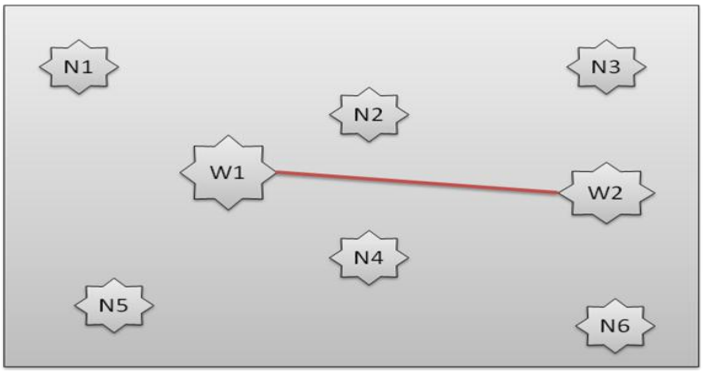

Fig. 3 Wormhole Attack

There are basically two kind of worm attack can be performed by attackers, Hidden mode attack and Exposed attack.

1) *Hidden Mode Attack:*

In this attack attacker do not expose his presence to the other nodes in the network. They also do not update packet header by their own MAC address as identity so that receivers can never aware about the existence of such node [6]. In fig. 3 the path from source to destination would be N1-N2-N6 because W1 and W2 are hidden in network [7].

2) *Exposed Mode Attack:*

In this attack, attackers include their identity in the packet header as legitimate node so other node aware about their presence but do not aware about their malicious intention [6]. In fig. 3 the path from source node N1 to destination node N6 would be N1-N2-W1-W2-N6 because they appear in the network as legitimate node [7].

Either Hidden or Exposed mode, the communication channel between malicious node is established using In-Band (I-B) or Out-Band (O-B) channel. In-Band channel tunnels the packet to each other through legitimate node in the network. Out-Band channel connects two malicious nodes via an external communication link such as network cable or wireless link [8].

B. *Blackhole Attack*

In this attack, a malicious node advertises valid and shortest route to a victim node and thereafter secretly drops data and control packets as they pass through it. In order to have shortest route, blackhole creates forged packet by modifying hop count and sequence number of the routing protocol message such as AODV. As shown in fig. 4, the source node N1 wants to communicate with destination node N7. It broadcasts RREQ (route request) messages to its neighbors. An attacker N6 forges a reply packet by modifying hop count claiming that it has shorter route to N7 or by incrementing destination sequence number than the authentic value last advertised by N7 indicating it has fresher route to N7. This leads to the establishment of a fake route through the attacker when maliciously fabricated reply reaches N1 first than legitimate reply. So, attacker node can eavesdrop or drop the packets. Malicious node is known as blackhole since it consumes data packets forwarded to it and never forwards those [9].

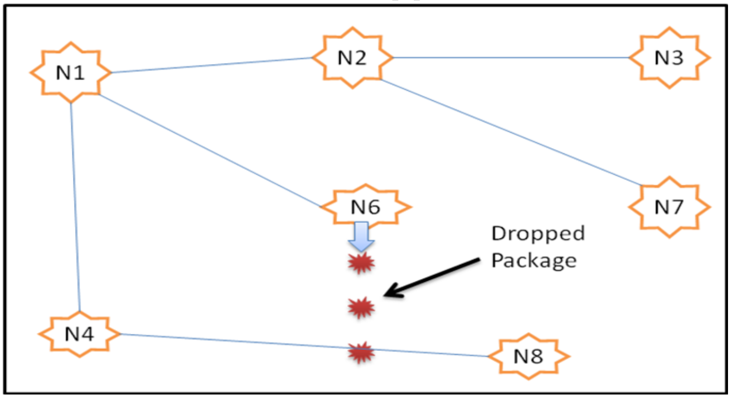

Fig. 4 Black hole Attack

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

1) *Internal Blackhole attack:*

This type of blackhole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node [10].

2) *External Blackhole attack* [10]*:*

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External blackhole attack can be summarized in following points

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update routing table.
- New route selected by source node for selecting data.
- The malicious node will drop now all the data to which it belong in the route.

C. *Byzantine Attack*

This attack involves multiple attackers that work in collusion to degrade the network performance such as creating loops, selectively dropping packets, choosing non optimal paths for packet forwarding [11]. In Fig 5, attacker N2 forwards routing packets of N1 (Source) normally to N3 but attacker N2 drops or forges these routing packets.

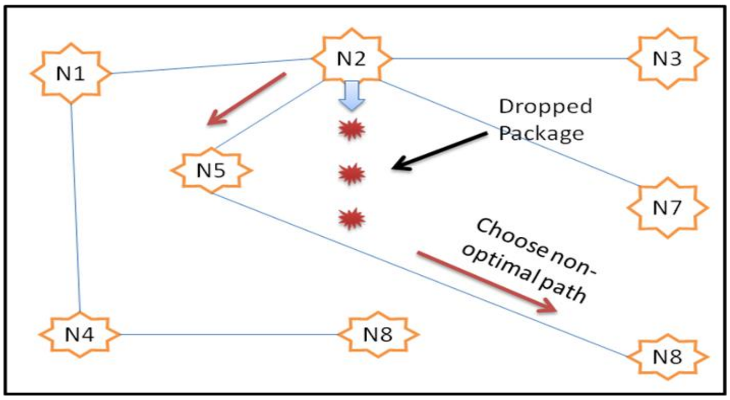

Fig. 5 Byzantine Attack

D. *Information Disclosure*

A compromised node may violate the confidentiality principle of security and disclose important information like private and public keys, status of nodes, passwords, optimal route to authorized nodes, geographic location of nodes and other control data in packet headers to unauthorized nodes present in the network. The location information revealed give better understanding of the network topology. Routing packets are then sent with inadequate hop-limit and ICMP error messages returned by the intermediate nodes are recorded. So it gives blueprint of the network i.e. which nodes are situated in close proximity to the target node [5].

E. *Routing Attack*

1) *Routing Table Overflow:*

This attack prevents creation of new legitimate routes by overflowing the routing table with routes to nonexistent nodes. This exploits the limited memory capacity of mobile nodes. A malicious node initiates route discovery to non-existent nodes so that limited memory of mobile node gets consumed by having such entries in their routing table which in turn prevents the creation of new routes to authorized nodes in the network. The proactive ad hoc protocols are more prone to this attack because in such networks, routes to all the nodes are already stored before they are needed, in contrast to reactive protocols in which information is discovered when needed[5].

2) *Routing Table Poisoning:*

In this attack, malicious node sends fabricated routing update and error messages or modified legitimate updates to authorized nodes in the network. It may result in forwarding packets along sub optimal routes, congestion in the network, formation of loops or blackmail attack in which an attacker sends false route error messages against benign node in order to report benign node as malicious and thus launching denial of service attack against it. In on demand ad hoc protocols, like AODV and DSR, there is separate route maintenance phase to deal with broken routes as nodes move or fail. Let a node S has route to node D via nodes X, Y and Z. A malicious node M can send RERR message to Y spoofing node Z, indicating that link between Z and D is broken so Y deletes corresponding entry for D from its routing table and forwards it to X. So M can successfully prevent traffic between S and D [5].

3) *Routing Cache Poisoning*

Route cache is maintained by on demand protocols like DSR that stores the routes known to it by overhearing neighborhood transmissions in the recent past. A malicious node can launch DOS attack on any node by simply broadcasting spoofed packets with source routes to D via itself. Any neighboring node overhearing the packet transmission adds the route entry in their route cache [5].

4) Replay Attack

An attacker instead of modifying packet‘s contents just replay stale packets in order to exploit battery power, bandwidth and computational constraint of mobile nodes. It leads to congestion in the network and confusion among the routing nodes because of conflicting information, thus delaying packet delivery or preventing them from reaching destination[5].

5) Rushing Attack

This attack involves entire network traffic to pass through an attacker. The source node is unable to find any secure route without the attacker. Malicious node after receiving RREQ packet from initiating node reacts immediately and floods the network quickly with these packets before other nodes receiving the same RREQ can react. Nodes receiving legitimate RREQ packets assume them as duplicates and discard them. So every route established has attacker as one of the intermediate nodes [5].

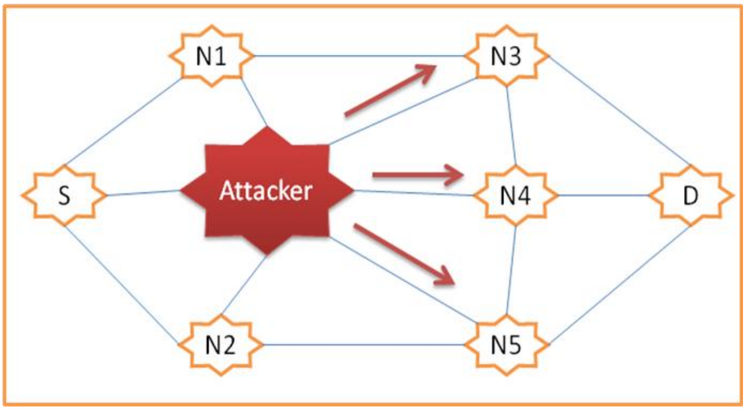

Fig. 6 Rushing Attack

As shown in fig. 6, when the source node S initiates the RREQ to the destination node D, if the RREQs are forwarded by a malicious node (Attacker), all the RREQs that come from attacker node will reach the destination D earlier than any RREQs that are forwarded by other nodes.

F. *Other Attacks*

1) Sinkhole:

A malicious node advertises fake routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated.

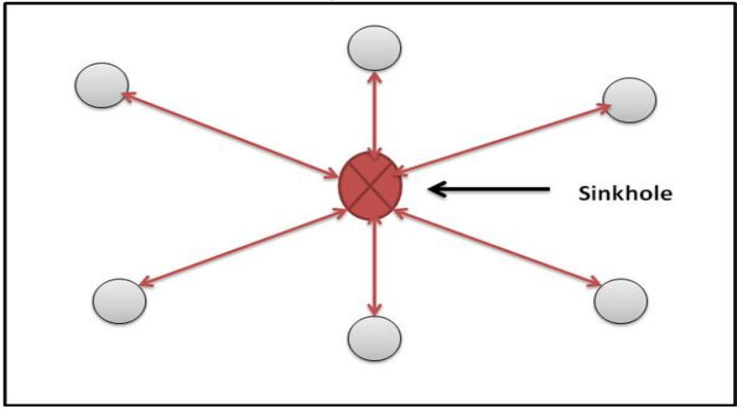

Fig. 7 Sinkhole Attack

Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop count. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate as shown in fig. 7. [12], [13].

2) Grayhole:

Grayhole simply drops packets coming from or destined to certain specific nodes in the network while forwarding all the packets for other nodes. Another type of Grayhole node behaves like maliciously for some time by dropping packets but may switch to normal behavior later. The Grayhole node does not drop all the packets coming to it but it drops the packets at a particular frequency so it is very difficult to detect as shown in fig. 8.

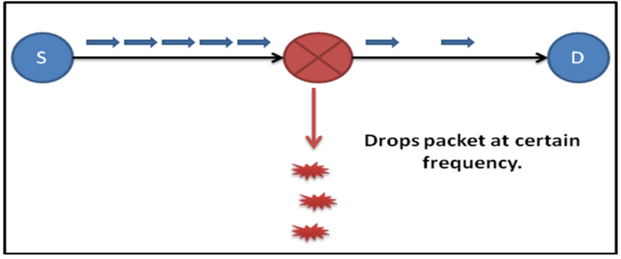

Fig. 8 Grayhole Attack

3) Sybil Attack:

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes as shown in fig. 9. The attacker may get access to all the data or may alter all packets in the same transmission so that the destination nodes cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party [12].

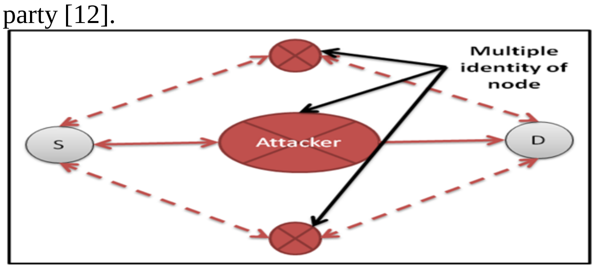

Fig. 9 Sybil Attack

4) Common Attacks on multi layers:

There are some malicious attacks which can be performed on all layers.

- Denial of Service Attack

Attackers simply make the entire system or services unavailable. It can also slow down the system by overloading the unnecessary resources or creating fake routing. As Adhoc network is decentralized by nature so that this attack can be launched against several layers i.e., signal jamming at physical layer, prevent channel access in link layer. On network layer, DOS attacks are performed on routing protocol and degrade the network performance by content modification; dropping packet and routing table overflow [14].

- Man in Middle Attack

Attacker sits between source and destination node and capture packet, modify content and also drop packet. The two communicating party does not aware about attacker who sits between them, they simply believe that they are communicating each other but actually they are communicating with man who sits at middle[11].

- Impersonate

Attacker steals identity of some legitimate node like IP or MAC address and pretends to a legitimate node and performs false routing, change the topology structure and many more malicious things [14].

V. SECURITY PRINCIPLES FOR MANET

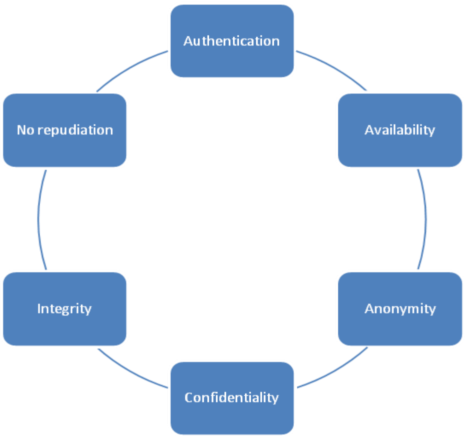

Fig. 10 Security Principles

A. *Security Principles*

1) *Authentication:*

The authentication must ensure that the only the legitimate sender and receiver can encrypt and decrypt a message. Authentication ensures that both the communicating entities must identify each other. Authentication is violated by impersonate attack in which malicious node steals someone's identity and act like a valid node.

2) *Availability:*

Availability ensures that resources or services must be available at all time when needed. Availability is often violated by attacker using denial of service attack.

3) *Anonymity:*

Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

4) *Confidentiality:*

Confidentiality ensures that only sender and receiver can share information no one else. Confidentiality can be achieve using secret key which is shared between two legitimate parties and also can be achieved using public or private key. Confidentiality is violated using eavesdropping and traffic analysis.

5) *Integrity:*

Integrity means that the content of message must not altered by unauthorized person. Integrity is violated using modification attack.

6) *No repudiation:*

No repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message.

B. *Framework Required for Secure MANET*

1) Confidentiality:

To achieving Data Confidentiality in a mobile ad hoc network, there should provide further protection to secret messages from being compromised or eavesdropped when they are delivered across the insecure network. The basic idea is to transform a secret message into multiple shares by private (secret) key cryptographic schemes and then deliver these shares of secret message via multiple independent paths to the destination so that even if any node that is assumed to be used to relay the message shares is compromised, the secret message as a whole is not compromised. [15]

2) Authentication and Non-repudiation:

Each node in an ad-hoc network has a key pair to use digital signature from asymmetric cryptographic system. The job of such nodes is now to verify securely the association between the address of a given ad hoc node and the public key of that node. Here digital signatures are useful to authenticate the messages, and hash chains to secure the hop count information, A neighbor node is informing to another node that it is not going to be able to route messages to certain destinations anymore, thus each and every node which is generating or forwarding a route error message uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature [15].

3) Data Integrity:

In Mobile Ad-hoc Network where ever node can participate. But there is a problem, that, how to trust the other nodes? How do we force every node in the network to be honest? We can only believe routing information. But this belief will fail if the source of such information is the destination of the route (in such a way that if you lie (since you can only lie about yourself) the only effect you get is that some other node can no longer communicate with you. With this scenario in mind, the best option could be to use an asymmetric cryptographic system which uses public and private key pairs so that the source of the route messages signs the message. It would not be needed to encrypt the routing messages because they are not secret. The only requirement is that the nodes will be able to detect forged routing messages [15].

VI. Conclusion

In this paper we have study MANET routing with comparisons among various protocol under different categories. We have also analysed various security attacks which are performed on network layer. We summarize here certain important point. First attacks on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination and node impersonation. All these mean that a wireless ad-hoc network will not have a clear line of defence and every node must be prepared for encounters with an adversary directly or indirectly. Second, mobile nodes are autonomous units that are capable of roaming independently. This means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked. Since tracking down a particular mobile node in large scale ad hoc networks may not be easily done, attacks by a compromised node from within the network are far more damaging and much harder to detect. Therefore, mobile nodes and the infrastructure must be prepared to operate in a mode that trusts no peer. Third, decision-making in mobile computing environment is sometimes decentralized and some wireless network algorithms rely on the cooperative participation of all nodes and the infrastructure. The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms. We studied security principles and present security framework model which required for MANET.

REFERENCES

[1] Sunil Taneja and Ashwani Kush, "*A Survey of Routing Protocols in Mobile Ad Hoc Networks*," International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[2] Bimal H Patel, Parth D Shah, Harikrishna B and Nishidh Chavda, "*Issues and Imperatives of Adhoc Networks*," International Journal of Computer Applications (0975 – 8887), Volume 62– No.13, January 2013.

[3] Geethu Mohandas, Salaja Silas and Shini Sam, "*Survey on Routing Protocols on Mobile Adhoc Networks*," 2013 IEEE.

[4] Namrata Marium Chacko, Shini Sam and P.Getzi Jeba Leelipushpam,"*A survey on various privacy and security features adopted in MANETs routing protocol*," 2013 The IEEE.

[5] Tarunpreet Bhatia and A.K Verma, "*Security Issues in MANET: A Survey on Attacks and Defense Mechanisms*," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3,issue 6,june 2013.

[6] V. Karthik Raju and K. Vinay Kumar, "*A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks*," 2012 International Conference on Computing Sciences.

[7] Poonam Dabas and Prateek Thakral, *"Detection and Prevention of Wormhole Attack in MANET: A Review*" International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 3, March 2013.

[8] Jonny Karlsson, Laurence S. Dooley and Göran Pulkkis "*A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis*" Sensors 2011, 11, 11122-11140; doi:10.3390/s111211122

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao "*A survey of black hole attacks in wireless mobile ad hoc networks*", Tsenget al. Human-centric Computing and Information Sciences2011,1:4 http://www.hcis-journal.com/content/1/1/4.

[10] Irshad Ullah and Shoaib Ur Rehman, "*Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols,*" Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010.

[11] Priyanka Goyal, Sahil Batra and Ajit Singh, "*A Literature review of security attack in mobile ad-hoc networks,*" International Journal of Computer Application (0975-8887), Vol. 9- No.12, Nov 2010.

[12] Kuldeep Sharma, Neha Khandelwal and Prabhakar .M, "*An Overview of security problems in MANET*," IEEE.

[13] Gagandeep, Aashima and Pawankumar, "*Analysis of Diffenrent Security Attacks in MANETs on Protocol Stack A-Review*," International journal of Engineering and Advanced Technology (IJEAT) Vol. 1, Issue 5, June 2012.

[14] Rachika Gupta, "*Mobile Adhoc Network (MANETS): Proposed solution to security related issues*," Indian journal of computer science and Engineering (IJCSE), Vol. 2 No. 5 Oct-Nov 2011.

[15] Prof. Mahedra Kumar Verma, Prof. Shubham Joshi and Prof. Nitika Vats Doohan, "*A Survey on: An Analysis of Secure Routing of Volatile Nodes in MANET*," IEEE.