IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol. 2, No. 1, 2012

Security Threats in Mobile Adhoc Network: A Review

Tanu Preet Singh
Department of Computer Science and Engineering
Amritsar College of Engineering and Technology
Amritsar, India

Satinder Kaur
Department of Computer Science & Engineering
Amritsar College of Engineering and Technology
Amritsar, India

Vikrant Das
Department of Computer Science and Engineering
Amritsar College of Engineering and Technology
Amritsar, India

Abstract: **A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi-hop network. The wireless nature of MANET gives the security to the designers, although security problems in MANETs give more attention but in last some days researchers have find out many types of attacks and system security, which means how to give security to the system.[2].Some fundamental characteristic are there such as open medium, dynamic topology, dynamic medium lead to the vulnerabilities. Whenever there is need to find the shortest path, the routing protocol does not give the shortest path but also give the path where we can travel fast. The routing Protocol which gives the shortest path it gives more collisions and delay in between. In order to avoid all loss in performance and gives less chance to collision this paper gives some techniques to discover the active shortcuts and best possible path .[3]**

Keywords: Security, route, MANET, Terminal, protocols.

I. INTRODUCTION

The people's future living environments are emerging based upon information resource provided by the connections of various communication networks for users. New small devices like Personal Digital Assistants (PDAs), mobile phones, handhelds, and wearable computers enhance information processing and accessing capabilities with mobility. Moreover, traditional home appliances, e.g. digital cameras, cooking ovens, washing machines, refrigerators, vacuum cleaners, and thermostats, with computing and communicating powers attached, extend the field to a fully pervasive computing environment. With this in view, modern technologies should be formed within the new paradigm of pervasive computing, including new architectures, standards, devices, services, tools, and protocols. Mobile networking is one of the most important technologies supporting pervasive computing. During the last decade, advances in both hardware and software techniques have resulted in mobile hosts and wireless networking common and miscellaneous. Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other:

Infrastructure- Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, UMTS, WLL, WLAN, etc. [4].

Infrastructureless- As to Infrastructureless approach, the mobile wireless network is commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system.

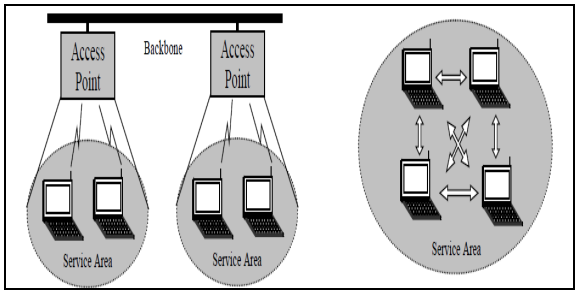

Figure1: Approaches of MANET

In this Paper, we describe the fundamental problems of ad hoc networking by givingrelated research background including the concept, features, status and applications of MANET. Some of the technical challenges MANET poses are also

presented based on which the paper points out the related kernel barrier. Some of the key research issues for ad hoc networking technology are discussed in detail that are expected to promote the development and accelerate the commercial applications of the MANET technology.

II. RELATED WORK

A. MANET Concept

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructured wireless network, including:

1) *Peer-to-Peer***.** Communication between two nodes which are within one hop. Network traffic (Bps) is usually consistent.
2) *Remote-to-Remote***.**Communication between two nodes beyond a single hop but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.
3) *Dynamic Traffic*. This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.[4]

B. MANET Features

MANET has the following features:
1) *Autonomous terminal***.** In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
2) *Distributed operation.* Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.
3) *Multihop routing.* Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
4) *Dynamic network topology.* Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).
5) *Fluctuating link capacity.* The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.
6) *Light-weight terminals.*In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions[4].

C. MANET Applications

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Adhoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

1) *Military battlefield.* Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of common place network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field [4].
2) *Commercial sector.* Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue

operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3) *Local level.* Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft,mobile ad hoc communications will have many applications.
4) *Personal Area Network (PAN).* Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.[4]

III. PROPOSED SYSTEM-ROUTING PROTOCOLS AND ATTACKS

Routing protocols are usually engaged to determine the routes following a set of rules that enables two or more devices to communicate with each other. In an ad hoc network routes are enabled in between the nodes using multi-hop, as the propagation range of the wireless radio is limited. The nodes engaged in traversing the packets over MANET are not aware of the topology of the network. Routing protocols discovers the topology by receiving the broadcast messages from its neighboring nodes in the network and respond to accordingly. Routing protocols are classified based on the different routing strategies.

- Pure distance vector algorithms are followed by the protocols Distributed Bellman Ford, Routing Internet Protocol. Due to the poor result of these algorithms new protocols are proposed with improvement enhancing the current algorithms, such as Least Resistance Routing (LRR), Distance Sequence Distance Vector (DSDV) protocol and Wireless Routing Protocol (WRP).
- Link state algorithms are used in the protocols Fisheye State Routing (FSR) protocol, Global State Routing (GSR) protocol, Optimized Link State Routing (OLSR) protocol, Source Tree Adaptive Routing (STAR) protocol etc.
- On demand routing protocols find routes on demand i.e., when traffic arrives to the protocol for routing. No prior routes are configured and it is not necessary to exchange the routing tables frequently. A route request packet is used by source to find a route before communication is initiated. The best route is found by a route selection algorithm. Several protocols follow this strategy i.e., Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), temporarily Ordered Routing Algorithm (TORA), Lightweight Mobile Routing (LMR) etc.
- Global Positioning System (GPS) in this routing algorithm protocols use the position of the nodes in traversing the packets. Protocols using this routing algorithm are Flow Oriented Routing Protocol (FORP), Distance Routing Effect.

A. Routing Protocols

A.1. Proactive (table driven) Routing Protocols

Proactive routing protocols maintain the routing information of all the participating nodes and update their routing information frequently irrespective of the routing requests. Proactive routing protocols transmit control messages to all the nodes and update their routing information even if there is no actual routing request. This makes proactive routing protocols bandwidth deficient, though the routing itself is simple having this prior updated routing information. The major drawback of proactive protocols is the heavy load created from the need to flood the network with control messages.

A.2. Reactive (On demand) Protocols

Reactive protocols establish the route only when it is required unlike the proactive protocols these protocols do not update their routing information frequently and will not maintain the network topology information. Reactive protocols use the connection establishment process for communication.Few pitfalls are noticed in these reactive protocols such as these are generally having high latency in searching the network. In finding the routes if there is excessive flooding over the network with route request packets it may result in network clogging.

A.3. Dynamic Source Routing (DSR) protocol

Dynamic source routing protocol (DSR) is a reactive protocol that is known as simple and efficient, specially designed for the multi-hop mobile ad hoc network. Often called “On-demand” routing protocol as it involves determining the routing on demand unlike the pro- active routing protocols that has periodic network information. Network nodes use multiple- hops to communicate, DSR protocol plays a key role in determining and maintaining all the routing automatically as the number of hops needed changes at any time and the mobile nodes involved may leave or join the network. DSR protocol

involves two major mechanisms to establish the routing process. These are route discovery and route maintenance.

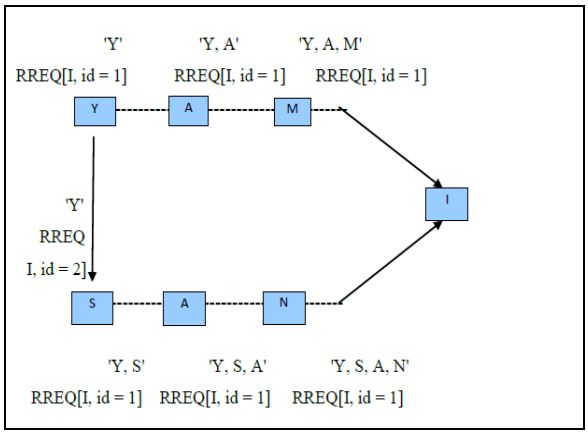

Figure 2: Route Discovery

B. Route Discovery

Route discovery is the process of DSR uses to find the route and to transmit the data from a source to destination where the source node is unaware of the destination route. For example, in fig 3.1

Let us assume node 'Y' wants to establish a route to node 'I'.

- Initially node 'Y' transmits 'RREQ' (Route Request) will usually be received by all the participating nodes in the network.
- This Route request contains information about the source and the destination along with unique request identification (id = 1 and id = 2 respectively in the considered figure).
- RREQ even maintains the information about all the intermediate nodes passed by while reaching the destination.
- Once the destination receives the RREQ packet then it will send the 'RREP' (Reply Route) to the source node 'Y'.
- RREP contains a copy of the route information of the RREQ then the source cache information to use in further communication process.

C. Route Maintenance

DSR protocol implements the route maintenance mechanism while communicating the packets from source to destination. But when the communication link between the source and the destination is broken or else a change in network topology is noticed. It will lead to failure of the communication between source node and destination node. In this scenario DSR protocols uses the route mechanism, to detect any other possible known route towards the destination to transmit data. If the route maintenance fails to find an alternative known route to establish the communication then it will invoke the route discovery to find the new route to destination.

***Disadvantage*:**

One of the major disadvantages of DSR protocol is an implementing the route discovery process. Source will transmit the RREQ messages to all the neighboring nodes to find the route to destination. It is fair and good when there are few nodes in the network, it will easily find a route and it can receive a RREP message from the desired destination. But if in case the network size is very high and participating nodes are numerous, then there will be a possibility to have so many routes to the destination. It may result in the reply storms this may cause collision of packets and it may increase the congestion at the nodes while sending reply.

Optimized Link State Routing (OLSR) protocol

OSLR protocol is a proactive protocol used in mobile ad-hoc networks. It is often called table-driven protocol as it maintains and updates its routing table frequently.

OLSR exchanges the topology information always with other nodes. Few nodes are selected as MPRs (Multi point relays). MPRs are responsible for transmission of broadcast messages during flooding and generating link state information. MPRs technique used in OLSR protocol will reduce the message overhead and even minimize the number of control messages flooded in the network. Nodes maintain the information of neighbors and MPR's, by sending and receiving HELLO messages from its neighbors. This will help in determining the link formation illustrated in the fig 3.

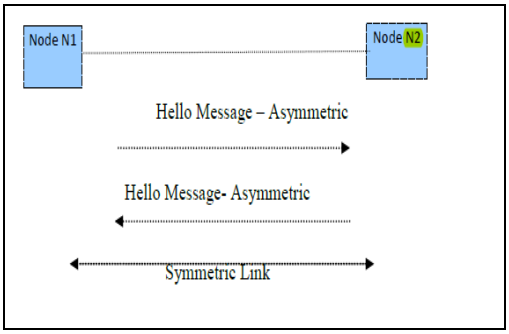

Figure 3: OLSR Symmetric link formation

- Node N1 transmits the HELLO message to node N2 and then the message received by node N2 from node N1 can be called asymmetric link.
- If this HELLO message is retransmitted by the node N2 to node N1 then the resulting link even called as asymmetric link.
- Finally the resulted bidirectional link is known as a symmetric link.
- Symmetric link formation will help the nodes to choose MPRs.

- MPRs will send the topology control (TC) messages containing the information about link status and MRP node information.

Ad Hoc On -Demand Distance vector (AODV)

Mobile nodes in the ad hoc network are dynamic and they use multi-hop routing by using Ad-Hoc On-Demand Distance Vector algorithm. AODV will not maintain the routes unless there is a request for route. Mobile nodes respond to the any change in network topology and link failures in necessary times. In case of the link failures the respective defective nodes are notified with the message, and then the affected nodes will revoke the routes using the lost link. This will help AODV to avoid the Bellman-Ford "counting to infinity" problem and then its operation is known as loop-free.
AODV uses Destination Sequence Numbers (DSN) for every route entry. DSN is created by the destination this DSN and the respective route information have to be included by the nodes while finding the routes to destination nodes. Routes with the greatest DSN are preferred in selecting the route to destination. AODV uses the message types Route Request (RREQ), Route Replies (RREP) and Route Error (RERR) in finding the route from source to destination by using UDP (user datagram protocol) packets. A typical AODV protocol follows the following procedure while routing.

- A source node intending to communicate to a destination it generally uses the RREQ constituting the source address and the broadcast ID address to its neighboring nodes to find the route to destination,
- This broadcast ID is incremented for every new RREQ. Once neighbors notice a destination route it will respond with RREP to the source.
- If the destination route is not found then it will re-broadcast the RREQ to its corresponding neighboring nodes by incrementing hop count.
- In this process a node participating in communication may receive the numerous copies of the broadcast packets in the pool of transmissions from all the corresponding nodes

Then the node cross check the broadcast ID of the request if the broadcast ID is new and have not received so far by the particular node then it will process the request if not the node drops down the superfluous RREQ and avoids the rebroadcast.

D. Security Services

The ultimate goals of the security solutions for MANETs is to provide security services, such as availability, confidentiality, integrity, authentication, nonrepudiation, anonymity to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in MANETs. The common security services are described below.

1) ***Availability***

Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or services of a distributed system. Availability ensures the survivability of network services despite of various attacks. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service.

2) ***Confidentiality***

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Release of such information to enemies could have devastating consequences e.g. *ENIGMA*. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield. With respect to the release of message contents, several levels of protection can be identified.

3) ***Integrity***

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service.

4) ***Authentication***

Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without

authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes.

5) Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. Nonrepudiation is useful for detection and isolation of compromised nodes. When node *A* receives an erroneous message from node *B*, nonrepudiation allows *A* to accuse *B* using this message and to convince other nodes that *B* is compromised.

6) Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system. It is very easy to make an island-hopping attack through one rough point in a distributed network.

E. Attacks in MANET

The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current *MANETs* are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. We have classified the attacks as modification, impersonation, fabrication, wormhole and lack of cooperation. [3]

E.1. Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct *DoS*attacks by modifying message fields or by forwarding routing message with false values. In ***fig4***, ***M*** is a malicious node which can keep traffic from reaching ***X*** by continuously advertising to ***B***a shorter route to ***X*** than the route to ***X*** that ***C*** advertises.

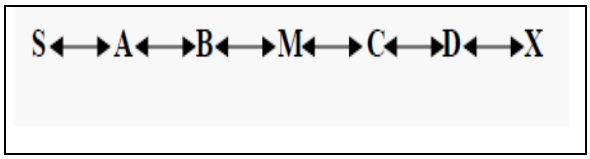

Figure 4: Ad hoc network and a malicious node

In this way, malicious nodes can easily cause traffic subversion and denial of service *(DoS)* by simply altering protocol fields: such attacks compromise the integrity of routing computations. 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.

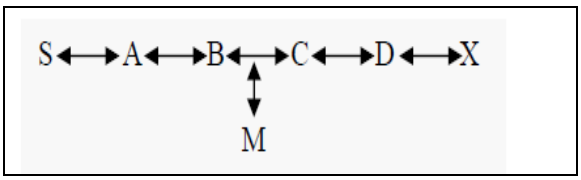

Figure 5: Ad hoc network with Dos attack

S transmits a data packet toward ***X*** with the source route ***S*** -->***A*** -->***B*** -->***M*** -->***C*** -->***D*** -->***X*** contained in the packet's header. When ***M*** receives the packet, it can alter the source route in the packet's header, such as deleting ***D*** from the source route. Consequently, when ***C*** receives the altered packet, it attempts to forward the packet to ***X***. Since ***X*** cannot hear ***C***, the transmission is unsuccessful.

E.2. Attacks Using Impersonation

As there is no authenticationof data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here we have described the scenario in details. [3]

A can hear ***B*** and ***D***, ***B*** can hear ***A*** and ***C***, ***D*** can hear ***A*** and ***C***, and ***C*** can hear ***B***, ***D*** and ***E***. ***M*** can hear ***A***, ***B***, ***C***, and ***D*** while ***E*** can hear ***C*** and next node in the route towards ***X***. A malicious node ***M*** can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination ***X***. At first, ***M*** changes its MAC address to match ***A***'s, moves closer to ***B*** and out of the range of ***A***. It sends a message to

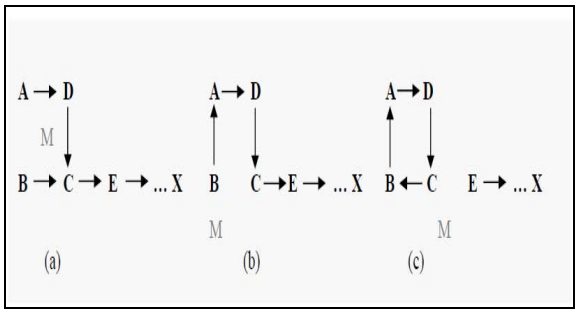

Figure 6: A sequence of events forming loops by spoofing packets. In the above fig 6. (b), there exists a path between five nodes.

B that contains a hop count to ***X*** which is less than the one sent by ***C***, for example *zero*.
Now ***B*** changes its route to the destination, ***X*** to go through ***A*** as shown in the *fig 6(b).* Similarly, ***M*** again changes its *MAC* address to match ***B***'s, moves closer to ***C*** and out of the range of ***B***. Then it sends message to ***C*** with the information that the route through ***C***ontains hop count to ***X*** which is less than ***E***. Now, ***C*** changes its route to ***B*** which forms loop as shown in *fig. 6(c).* Thus ***X*** is unreachable from the four nodes in the network.[3]

E.3.Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In *MANET*, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted. Consider the figure 7.
Suppose node ***S*** has a route to node ***X*** via nodes ***A***, ***B***, ***C***, and ***D***. A malicious node ***M*** can launch a denial-of-service attack against ***X*** by continually sending route error messages to ***B*** spoofing node ***C***, indicating a broken link between nodes ***C*** and ***X***. ***B*** receives the spoofed route error message thinking that it came from ***C***. ***B*** deletes its routing table entry for ***X*** and forwards the route error message on to ***A***, who then also deletes its routing table entry. If ***M*** listens and broadcasts spoofed route error messages whenever a route is established from ***S*** to ***X***, ***M*** can successfully prevent communications between ***S*** and ***X.***

E.4. Wormhole Attacks

Wormhole attack is also known as tunneling attack. 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. In the figure3.7***M1*** and ***M2*** are two malicious nodes that encapsulate data packets and falsified the route length [3].

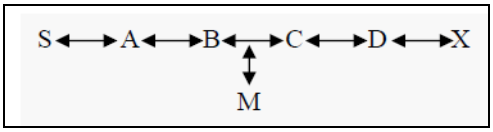

Fig 7: Adhoc Network with attack

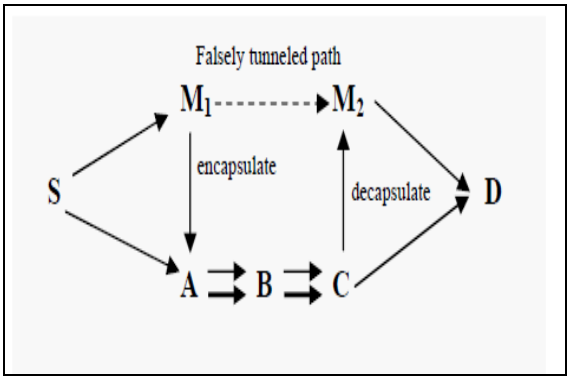

Figure 8: Path length spoofed by tunneling

Suppose node ***S*** wishes to form a route to ***D*** and initiates route discovery. When ***M1***receives a *RREQ* from ***S, M1*** encapsulates the *RREQ* and tunnels it to ***M2*** through an existing data route, in this case {***M1*** -->***A*** -->***B*** -->***C*** -->***M2***}. When ***M2*** receives the encapsulated *RREQ* on to ***D*** as if had only traveled {***S*** -->***M1*** -->***M2*** -->***D***}. Neither ***M1*** nor ***M2*** update the packet header. After route discovery, the destination finds two routes from ***S*** of unequal length: one is of 5 and another is of 4. If ***M2*** tunnels the *RREP* back to ***M1***, ***S*** would falsely consider the path to ***D*** via ***M1*** is better than the path to ***D*** via ***A***. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

E.5. Lack of Cooperation

Mobile Ad Hoc Networks *(MANETs)* rely on the cooperation of all the participatingnodes. The more nodes cooperate to transfer traffic, the more powerful a *MANET* gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack[3].

CONCLUSION

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to

deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this report, we have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. The first research question is 'what are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?' In our study, we present a variety of attacks related to different layers and find that network layer is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. 'How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?' is the second research question. The answer is that security services can be achieved through following the preventive and reactive countermeasures on the basis of particular attack. The third question is 'what are the countermeasures? How the security of the entire system is ensured?' we focus on the potential countermeasures either currently used in wired or wireless networking or newly designed specifically for MANET in our study. In addition, we can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. The final research question is 'what are the potential dangers that may be crucial in future?' Every day, the attackers are trying to find out the new vulnerability in MANET.

IV. FUTURE SCOPE

Significant research in MANET has been ongoing for many years, but still in an early stage. Existing solutions are well-suited only for specific attack. They can cope well with known attacks but there are many unanticipated or combined attacks remaining undiscovered. Resource consumption DoS attack is still unclear to the researchers. More research is needed on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Existing routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of service attack. So, necessity of secure routing protocol is inevitable. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management. The public cryptography scheme depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET. Symmetric cryptography is efficient but suffers from potential attack on key distribution. Hence, efficient key agreement and distribution in MANET is an ongoing research area. Finally, Building a sound trust-based system and integrating it to the current preventive approaches, solution of the node selfishness problem can be considered in future research. Identifying new security threats as well as new countermeasures demands more research in MANET.

REFERENCES

[1] ArtiSehgal ,RuplaiAhuja, Sunil Kumari " A security architecture for mobile Ad hoc Networks" Proc. of the International Conference on Science and Engineering (ICSE 2011) Copyright © 2011 RG Education Society ISBN: 978-981-08-7931-0

[2] ShuyaoYu,YoukunZhang,Chuck Song, Kai Chen " A security architecture for mobile Adhoc networks" preceding in Institute of Computing Technology, School of Software, 1999

[3] Nishugarh and R.P.Mahapatra " MANET security issues" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009

[4] Jun-Zhao "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing" in IEEE communication magazine vol.3 pp. (316-321)2001

[5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks", Proc. Ninth Int'l Conf. Network Protocols(ICNP), Nov. 2001.

[6] J-P. Hubaux, L. Buttyan and S. Capkun: The Quest for Security in Mobile Ad Hoc Networks, Proceedings of the 2nd ACM MobiHOC, 2001.

[7] L.Buttyan, J. Hubaux Enforcing Service Availability in Mobile Ad-Hoc WANs, 1st IEEE/ACM workshop on Mobile Ad Hoc Networking and Computing, 2000.

[8] L. Zhou and Z. Hass, "Securing Ad Hoc Networks" , IEEE network, vol. 13, no.6 pp24-30, 1999. [9] P. Papadimitratos, Z. Haas, Secure routing for Mobile Ad Hoc Networks, Proceedings of CNDS , 2002.

[9] P. Papadimitratos, Z. Haas, Secure Data Transmission in Mobile Ad Hoc Networks, ACM Workshop on Wireless Security, 2003.

[10] S. Bonum, J.Ben-Othman, Data Security in Ad Hoc Networks Using MultiPath Routing, Proc. 14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, 2003.

[11] S. Capkun, L. Buttyan, J. Hubaux: Self-Organized Public- Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, VOL.1, NO.1, 2002.

[12] S. Marti, T. Giuli, K.Lai and M.Baker: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, the 6th MobiCom 2000.

[13] T. Gross, J.-P. Hubaux, J.-Y. Le Boudec and M. Vetterli: Toward Self-Organized Mobile Ad Hoc Networks: The Terminode Project", IEEE Communication Magazine, vol.39, issue 1, pp. 118-124, 2001.

[14] W. Lou, W. Liu, Y. Fang: SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, IEEE INFOCOM, 2004.

[15] Y. Hu, D.Johnson, A. Perrig: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Proc. IEEE workshop on Mobile Computing Systems and Applications, 2002.

[16] Y. Zhang, W. Lee: Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the 6th MOBICOM 2000