International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196

Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture

Ajay Jangra[1], Nitin Goel[2], Priyanka[3] & Komal Bhatia[4]

[1, 2]CSE deptt. U.I.E.T. Kurukshetra University, Kurukshetra, India.
[3]ECE deptt. Kurukshetra Institute of Technology and Management, Kurukshetra, India.
[4]CSE deptt Y.M.C.A. University of Science and Technology, Faridabad, India.

Abstract: Mobile ad hoc networks have inherently different properties than traditional wired network. Mobile ad hoc networks (MANETs) have received drastically increasing interst, partly owing to the potential applicability of MANETs to myriad application. Security is a paramount concern in a mobile ad hoc network because of its intrinsic vulnerabilities. In this paper we review security goal, security challenges, and different types of attacks on MANETs and also try to propos the solution to diffent security threats at layer wise by Reactive routing protocols. Basically we follow some reactive protocols like: Dynamic Source Routing(DSR), Ad Hoc on demand Distance Vector Routing (AODV) and Temporally Ordered Routing Algorithm(TORA). However, we can say that how these protocols can be secured.

Keywords/Index Terms: MANET, Security, Attack Prevention, Secure Routing, Vulnerabilities

INTRODUCTION

With recent performance advancements in wireless communication technologies mobile wireless computing has become increasingly popular. Wireless network provide mobile users with ubiquitous communication capability and information access regardless of its location. The conventional wireless networks require centralized monitoring through a fixed infrastructure. Here every mobile mode in a communication cell can reach a base station in a single hop radio transmission.

In parallel with single hop network, another type of model based on radio to radio multi-hopping has been evolving to serve a growing number of applications which rely on fast developable multi-hope infrastructure less network. The classical examples are battlefield communication, disaster and recovery search and rescue operations etc. In the next generation of wireless communication systems, there is a tremendous need for the rapid deployment of independent mobile users. Significant examples include emergency search/ rescue missions, disaster relief efforts, mine site operations, battlefield military operations, electronic class-rooms, conferences, convention centers etc. A network of such users is referred to as Mobile Ad hoc Network (MANET). Such a network does not have any fixed infrastructure (i.e., no such base stations/routers); nodes arbitrarily change their positions resulting in a highly dynamic topology causing wireless links to be broken and re-established on-the-fly. [2, 9, 10]

Securing in wireless ad hoc networks has recently gain a momentum and became a primary concern in attempt to provide secure communication in a hostile wireless ad hoc environment. Numerous proposals were suggested without deriving a general solution. Securing a wireless ad hoc network is particularly difficult for many reasons including the:

- *Vulnerability of Channels:* Message can be eavesdropped and fake messages can be injected into the network, with no necessity of physical access:
- *Vulnerability of Nodes:* Nodes can be easily captured or stolen and can fall under the control of the attacker;
- *Absence of Infrastructure*: Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on-line servers;
- *Dynamically Changing Topology*: Sophisticated routing protocols designed to follow the permanent changes in topology can be attacked by incorrect routing information generated by compromised nodes, which is difficult to distinguish.

Now how Mobile Ad hoc networks generally works; how the nodes in MANETs are communicating and make a secure network. Fig.1 shows how it works.

SECURITY GOALS IN AD HOC NETWORKS

The security of communication in ah hoc wireless networks is important especially in military applications. The absence

*Corresponding Author: [1]er_jangra@rediffmail.com, [2]goelnitin0887@yahoo.com, [3]priyanka.jangra@gmail.com, [4]komal_bhatia1@yahoo.com

of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber attacks than wired networks[1,2,7].

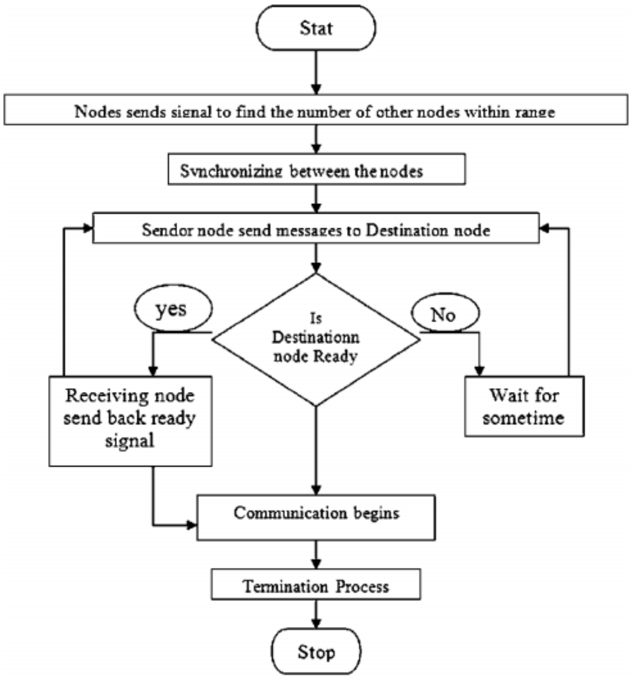
Stat
Nodes sends signal to find the number of other nodes within range
Synchronizing between the nodes
Sendor node send messages to Destination node
yes
Is Destinationn node Ready
No
Receiving node send back ready signal
Wait for sometime
Communication begins
Termination Process
Stop

Figure. 1: Working of a General Mobile Ad Hoc Network

The key attributes required to secure ah hoc network are:

1. *Confidentiality* ensures payload data and header information is never disclosed to unauthorized nodes.
2. *Integrity* ensures that message is never corrupted
3. *Availability* ensures that services offered by the node will be available to its users when expected, i.e. survivability of network services despite denial of service attacks.
4. *Authentication* enables a node to ensure the identity of peer mode it is communicating with.
5. *Non-repudiation* ensures that origin of a message cannot deny having sent the message.

SECURITY CHALLENGES

Achieving securing performances in wireless ad hoc environment is a challenging task. Unlike the wire-line networks the unique characteristics of ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer architecture, insecure operational environment and shared broadcast radio channel, stringent resource constraints, roaming of nodes, highly dynamic network topology combined with lack of central authority and association, scalability and physical vulnerability. [1, 11]

Roaming nodes with relatively poor physical protection can be exposed to malicious attacks by compromised nodes. To reduce the vulnerability, which may be caused by compromised centralized entity, and to achieve high survivability, ad hoc network should have distributed architecture.

Dynamic topology and changeable nodes membership may disturb the trust relationship among the nodes. The trust may also be disturbed if some nodes are detected as compromised. Nodes in wireless ad hoc networks may be dynamically affiliated to different administrative domains. This dynamism could be better protected with distributed and adaptive security mechanisms [11].

Scalability is an important issue concerning security. Security mechanisms should be capable of handling a large network as well as small ones [1].

Resource availability (band-width, battery and computational power) in ad hoc networking is a scarce feature. Providing secure communication in such changing and dynamic environment, as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad hoc environments also allow implementation of self-organized security mechanisms.

ATTACKS IN AD HOC NETWORKS

The security of communication in ah hoc wireless networks is important especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber attacks than wired networks. These attacks are generally classified into two types: Passive and Active attacks.

Passive attacks do not influence the functionality of a connection. An adversary aims to interfere in a network and read the transmitted information without changing it. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality is violated. It's difficult to recognize passive attacks because under such attacks the network operates normally. In generally, encryption is used to combat such attacks.

Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the ad hoc network are involved, the attacks are referred to as internal attacks.

In order to combat passive and active attacks a secure ad hoc network is expected to meet the following different security requirements [3]:as discussed in SECURITY GOALS of ad hoc wireless networks. Fig. 2 outlines different active attacks that have been used in the literature to study the performance of routing protocols corresponding to above described security requirements. We use these attacks along with the security requirements as a guide to revenue the salient passive, active, and hybrid routing protocols for MANETs.

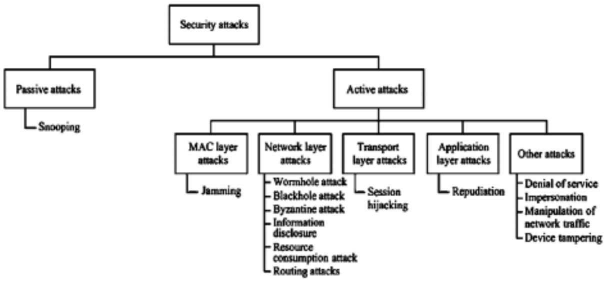

Figure 2: Classiûcation of Attacks in Wireless Ad hoc Networks

Black-Hole *(Network Layer Attach)*: All packets are dropped by sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them, or the attacker could cause the route at all nodes in an area of the network to point "into" that area when in fact the destination is outside the area.

Wormhole *(Network Layer Attach)*: Using a pair of attacker nodes A and B linked via a private network connection. Every packet that A receives from ad hoc network, A forwards through the wormhole to B, to then be rebroadcast by B, similarly, B may send all ad hoc network packets to A.

Malign *(Network Layer Attach)*: Watchdog and path-rather are used in ad hoc routing protocols to keep track of perceived malicious nodes in a blacklist. An attacker may blackmail a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.

Partition *(Network Layer Attach)*: An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another.

Detour *(Network Layer Attach)*: An attacker may attempt to cause a node to use detours through suboptimal routes. Also compromised nodes may try to work together to create a routing loop.

Routing Table Poisoning *(Network Layer Attach)*: The publication and advertisement of fictitious routes.

Packet Replication *(Network Layer Attach)*: The replication of sale packets, to consume additional resources such as bandwidth, etc.

Session Hijacking *(Transport Layer Attach)*: One weak point is that most authentications processes are only carried out once when a session starts. An adversary could try to appear as an authentic node and hijack the session (Transport Layer Attack).

Dos: An adversary tries to disturb the communication in a network, for example by flooding the network with a huge amount of packages. Service offered by the network are not working as usual, slow down or even stop. Ad hoc wireless Networks are more affected than wired networks, because there are more possibilities to perform such an attack

***Jamming (MAC Layer Attach)*:** An adversary sends signals with the same frequency in that a sender and receiver communicates what cause a lot of errors in the transmission.

Table1
Security Solution for MANETs [1]

Layer	*Security Issues*
Application Layer	Detecting and preventing Viruses, worms, malicious codes, and applications abuses.
Transport Layer	Authentication and Securing end-to-end communication through data encryption
Network Layer	Protecting the ad hoc routing and forwarding protocols
Link Layer	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Preventing Signal jamming, denial-of-service attacks

SECURE AD HOC ROUTING PROTOCOLS

Routing in ad hoc networks has been an active research area and in recent years numerous routing protocols have been introduced for MANETs. The deployment of such networks still faces challenges, such as limited physical security, mode mobility and limited resources (i.e., processor, power, bandwidth, storage). The major issues that affect the design, deployment, and performance of a MANET include: medium access scheme, routing, multicasting, transport layer protocol, pricing scheme, quality of service provisioning, self-organization, security, energy management, addressing and service discovery, scalability and deployment consideration. The protocol design issues are inherently related to the underlying ad hoc applications. Routing protocols are designed for purposes such as quality of service provisioning, energy management and security. [1,8,10,13]

CHALLENGES IN SECURE AD HOC ROUTING PROTOCOLS

Major challenges that a routing protocol designed for Ad Hoc wireless networks faces include: mobility of nodes, resource constraints, error-prone channel state, and hidden and exposed terminal problems [1,4,10].

- ***Mobility:*** The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes and the addition of new nodes to the network. Disruption in service may occur either due to the movement of the intermediate nodes in the path or due to the movement of the end nodes.

- ***Bandwidth Constraints***: In wireless networks, the capacity of the radio band is limited and hence the data rates it can offer are much less than what a wired network can offer. That is why the routing protocol should use the bandwidth optimally to keep the overhead as low as possible.
- ***Error-Prone Channel State*:** The wireless links have time-varying characteristics in terms of link capacity and link-error probability. This requires that the ad hoc wireless network routing protocol should interact with the MAC layer to find alternate routes through better quality link.
- ***Hidden Terminal Problem*:** Refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the recover.
- ***Exposed Terminal Problem*:** Refers to the inability of a node to transmit to another node when the wireless channel is not free due to transmission by the nearby transmitting node.
- ***Resource Constraints:*** Battery life and processing power are two essential and limited resources that form the major constraint for the nodes in ad hoc network. Thus, ad hoc wireless network routing protocols must optimally manage these resources.

Types of Ad Hoc Routing Protocols

Routing protocols for ad hoc wireless networks can be classified into three types based on the underlying routing information update mechanism employed. An ad hoc routing protocol could be:

1. Reactive (on demand);
2. Proactive (table driven); and
3. Hybrid.

***Reactive Protocol (on Demand)*:** Reactive routing protocols obtain the necessary path when it is required, by using a connection establishment process. They do not maintain the network topology information and they do not exchange routing information periodically. Reactive routing protocols often outperform proactive ones due to their ability to adjust the amount of network overhead created to track the mobility in the network.

***Proactive Protocol (Table Driven*)**: Proactive routing protocols, such as DSDV, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains. [10, 12, 13]

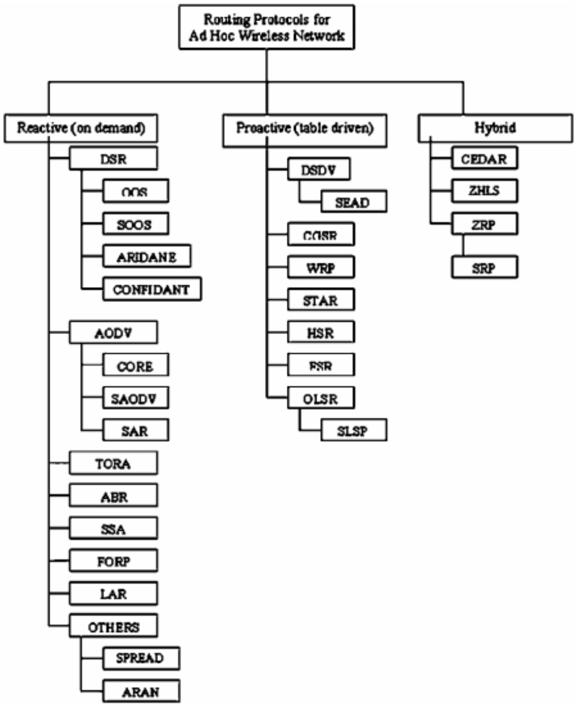

Figure 3: Types of Ad Hoc Routing Protocols

Hybrid Protocol: Hybrid routing protocols such as ZRP and SLSP combine the best features of both reactive and proactive routing protocols. For example, a node communicates with its neighbors using a proactive routing protocol, and uses a reactive protocol to communicate with nodes farther away. In other words, for each node, nodes within certain geographical are reached using proactive routing protocols. Outside the geographical area, reactive routing protocols will be used. [2]

REACTIVE ROUTING PROTOCOLS

Reactive routing protocols obtain the necessary path, when required, by using a connection establishment process. Such protocols do not maintain the network topology information and they do not exchange routing information periodically. We focus more on reactive routing protocols because they often outperform proactive ones due to their ability to adjust the amount of network overhead created to track the mobility in the network affecting current communication.

***Dynamic Source Routing Protocol*:** Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is *becon-less* and hence does not require periodic *hello* packet (*beacon*) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding *RouteRequest* packets in the network. The destination node, on receiving a *RouteRequest* packet, responds by sending a *RouteReply* packet back to the source, which carries the route traversed by the *RouteRequest* packet received. [1, 2,10]

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a *RouteReques*t packet. This *RouteReques*t is flood throughout the network. Each node, upon receiving a *RouteReques*t packet, rebroadcasts the packet to its neighbours if it has not forwarded already or if the node is not the destination node, provided the packet's time to live (TTL) counter has not exceeded. Each *RouteReques*t carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a *RouteReques*t packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate *RouteReques*t. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same *RouteRequest by* an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a *RouteReques*t packet during the route construction phase. A destination node, after receiving the first *RouteRequest packet*, replies to the source node through the reverse path the *RouteReques*t packet had traversed.[2,5]

No security issues have been introduced in the basic DSR configuration. Also the resource management is not utilized well. For example, if an intermediate node does not know the destination address, it forwards the *Route Request* message to all its neighbours.

***Qos-Guided Route Discovery*:** Maltz, introduced Qos-Guided route discovery protocol which allows a node to specify QoS metrics that must be satisfied by a discovered path. So, when a node needs to initiate a *RouteReuqest* it will look first in its cache route. If the route to the destination exists, the node may choose to use it. If the flow establishment is successful, it is not necessary to perform a QoS-Guided route discovery, although it may be performed in an attempt to find a better route. The decision about whether or not to perform such a discovery may be based on resources available along a preexisting route or it may be based on the nodes' estimate of the probability of successful flow along that route. A node may choose to always perform a second search requesting a slightly higher level of resources that is available along the preexisting route. [10,12,14]

Maltz is using the three traditional QoS metrics, bandwidth, latency and jitter. With the bandwidth metric, a node forwarding a packet updates the current resource level filed with the value that is lesser of the resource level that it received and its own resource level. For example, which a node with 240kb/s of available bandwidth receives a request with a current resource level of 640kb/s, it reduces the bandwidth level in the *RouteRequest* packet before forwarding it. For the metrics of latency and jitter, each mode actually increases the latency and jitter specified in the Request, and therefore, adds the local latency or jitter to the received value. [12,14]

Securing Quality of Service Route Discovery: SQoS is a secure form of Qos-Guided route discovery for an demand ad hoc network routing. SQoS relies entirely on symmetric cryptography. Symmetric cryptographic primitives are three to four orders of magnitude faster (in computation time) than asymmetric cryptography. [2]

SQoS builds on hash chains and MW chains. Hash function is simply a one way has function. If *X* is any random number, then $Y = H(X)$; where *H* is the hash function and there is no way to know *X* if you get *Y*. For example, instead of storing the user's password *X*, the system stores only the value $Y = H(X)$. The user identifies himself by sending *X* to the system; the system authenticates his identify by computing $H(X)$ and checking that it is equal to the stored value *Y*.

MW chain provides instant authentication and low storage overhead. MW chain is based on one time signature. One time signature works as follows. Each mode selects a private key K that is used to generate verification key V and signature S. If the node has a message to send, it will sign it using its signature S. Only nodes that have been communicated key V can read the message (note that node that has V, can not generate S). In this way we can sign each message with different S (derived from K), and verify it using either different V or in some cases the same V. [2]

ARIADNE: ARIADNE is a secure on-demand routing protocol which relies only on efficient symmetric cryptography and withstands compromised nodes. Ariadne authenticates routing messages using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures Ariadne uses TESLA, i.e. an efficient broadcast authentication scheme that requires loose time synchronization.[2,5]

The Ariadne protocol works in two stages i.e. it firstly verifies the authenticity of the RREQ, secondly then an efficient per-hop hashing technique is used to verify that no node is missing from the node list in the RREQ. The source node includes a message authentication code (MAC) computed with shared key. The destination/intermediate node verifies the RREQ authenticity and freshness using the shared key. Thereafter, the destination node authenticates each node in the node list of the RREQ so that it will return a RREP only along paths that contain legitimate nodes using TELSA key.

The salient features of Ariadne are that it can *handle nodes that can modify/fabricate routing information, combats against attacks such as impersonation, wormhole, copes against compromised nodes: RREQ flooding is avoided, etc*.

AODV: AODV is very similar to DSR. AODV works by sending a *RouteRequest* message to the destination. The source node and the intermediate nodes store the next hop information corresponding to each flow for data packet transmission. The major difference between AODV and other on demand routing protocols is that it uses a destination sequence number (DesSeqNum) to determine an up to date path to the destination. A node updates its path destination only if the DesSeqNum of the current packet received is greater than the last DesSeqNum stored at the node. The *RouteRequest* message carries six items; the source identifier, destination identifier, source sequence number, destination sequence number, broadcast identifier and time to live. [2,3]

AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or through ACK messages, the source and the destination nodes are notified (end nodes). The source node then re-establishes the route with the destination using higher layers.It is important to recognize the main differences among the DSR and AODV. DSR is a pure on-demand Ad hoc routing protocol. AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers and periodic beacons from DSDV.[2,3]. AODV does not provide any type of security. *Also the resource management is not utilized well. For example, if the intermediate node does not know the destination address, it will forward the* Route Request *to all the nodes*.

CORE: Each network entity keeps track of other entities collaboration using a technique called reputation. Three reputation systems are used in CORE: subjective reputation, indirect reputation and functional reputation. The subjective reputation is calculated directly from the subject observation. A subjective reputation (direct observation) at time t from the point of view of subject s is calculated using a weighted mean of the observation's rating factors, giving more relevance to the past observations. Indirect reputation reflects the value given to the final reputation by the characteristics of the complex societies. Functional reputation is used to apply a function f (which could be a forwarding function, packet function, or any other function) to the subjective reputation value or/ and the indirect value. The function reputation may apply more than one function to the same input and use a third function to get a final functional value.

CORE consists of three components: network entity, reputation table and the watchdog mechanism. The network entity comprises of the mobile nodes in the network. Each node is enriched with a set of Reputation Tables (RT) and a Watchdog Mechanism (WD). The RT and the WD together constitute the basis of the collaborative reputation mechanism.

SAR: The Security-aware Ad Hoc Routing Protocol (SAR) protocol can be incorporated in both on-demand and table-driven routing protocols. In SAR, a hierarchical level of security is designed by defining a level of trust as a metric for routing, i.e. different keys are used for each level [2,3,5]. Here, each node is associated with certain security level. Hence, a security metric is embedded into the RREQ packet. On receiving a RREQ packet, each intermediate node with a particular security metric or trust level compares it with that defined for the packet. The SAR ensures that this node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level. If the node cannot provide the required security, the RREQ is dropped. If an end-to-end path with the required security attributes can be found, a suitably modified RREP is sent from an intermediate to other source node. The major limitation of SAR is that it *lacks in scalability due to the existence of multiple trust levels where multiple keys are required to be generated and distributed*.

SAODV: The black-hole attack is a killer attack for AODV. In a black hole attacks a malicious node acts as an intermediate node, and advertises itself on the shortest path to the destination, which will make the sender node send all the packets through it. The malicious node will then simply drop the packets.

The approach adopted in SAODV is adequate for solving the black-hole problem but it fails to detect the wormhole attacks (when two malicious nodes works together to attack the network).

TORA: In TORA [2], routs are defined by a Directional Acyclic Graph (DAG), rooted at the destination node. To create the DAG, nodes use a height metric, consisting of five parameters: logical time of link failure, unique ID of the node defining the new reference level, reflection indicator bit, a propagation ordering parameter with respect to common reference level and unique ID of node. Three types of control packets are used: query (SRT), update (UPD), and clear (CLR). QRT messages are flooded to all intermediate nodes until the destination node is reached and upon which a UPD message is used to update nodes along with the reverse path from destination to source. UPD messages are also used to indicate link failure. A CLR broadcast is sent throughout the network to clear invalid routes.

As timing is an important factor within the height metric, synchronization of timing is important for effectively executing TORA routing. This is sometimes achieved through an external clock source such as GPS. However, not all mobile devices are GPS enabled, and, therefore, this routing protocol will pose a considerable challenge for wide spread deployment and inter-operability for heterogeneous mobile devices.

Table 2
Secure Aware Routing Propeties and Techniques [16]

Authenticity	Password, Certificate
Authorization	Credentials
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-repudiation	Changing of digital signature
Timeliness	Timestamp
Ordering	Sequence Number

Table 3
Defense Against Attacka [17]

Attack	*Targeted Layer in the protocol Stack*	*Proposed Solution*
Warmhole Attack	Physical and MAC	FHSS, DSSS
Blackhole Attack	Network	Packets Leashes
Resource Consumption	Network	SEAD[2]
Information Disclosure	Network	SMT[2]
Location Disclosure	Network	SRP[2], NDM[2]
Routing attacks	Network	SRP[2], SEAD[2],
Repudiation	Application	ARAN[2]
DOS	Multi-Layer	SEAD[2], ARIDANE[2]
Impersonation	Multi-Layer	ARAN[2]

Table 4
Security Feachures in Some of the Routings Protocols in Ad Hoc Networks [18, 19]

Protocols	*Security Positives*	*Security Negatives*
SRP	Fabricated, compromised or replay route replies rejected; No online CA; guaranteed acquisition of correct topological information in a timely manner; No complete knowledge of keys By all nodes	Security association as a requirement; possible attack when nodes collude during the two phase of a single route discovery; each SRP query can only discover routes should be set up to ensure robustness
SAR	Can be easily incorporated on different routing protocols; Defines different trust levels	Requirement for different keys for different level of trust (large number of keys); dynamic key
SEAD	Implements one-way hash chain which is a cheaper solution; uses Access node authentication; overcomes the DOS attacks	Sensitive to wormhole attacks
ARAN	Uses cryptographic certificates and robust against modifications, fabrication and Impersonation	Requires preliminary certification process; costly protocol due to asymmetric cryptography, not immune to wormhole attacks
ARIDANE	Uses symmetric cryptography and is based on authentication (Shared key, MAC and authentic route discovery chain); guarantees that the target node of a route discovery authenticates the source	Needs mechanism to bootstrep authentication keys; only the enhanced version protects against a wormhole attack
S-AODV	Public key cryptography used	High overhead; possible route Discovery corruption; compromise of IP portion
Sec-AODV	Uses SUCV, provides on-demand trust establishment	Sensitive to DOS attacks
SMT	Guarantees integrity, replay protection and origin authentication; interoperability with accepted procedures such as Source routing; symmetric key cryptography used	Limited protection against compromised topologcal information
OSPF	Flooding the information least dependency; hierarchy routing and information hiding; two authentication methods; a simple password scheme and a cryptographic message digest	Age field not protected by digital signature; internal routers can generate incorrect routing information; public key cryptogyaphy very expensive and will slow performance of the router

CONCLUSION

Mobile ad hoc Network have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. In this paper we have highlighted what kind of attacks are possible at different layers on MANETs, what are the different security goals, security challenges we need to follow while working/ designing the secured protocol for ad hoc wireless network. The proposed routing protocols should be highly secured from all types if vulnerabilities. By that any protocol and simulation to test them should include the capability to handle each node, known and unknown security threats.

REFERENCES

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhanng, "Security on Mobile Ad Hoc Networks: Challenges and Solutions" 1536-1284/04/IEEE Wireless Communications Feb., 2004.

[2] C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols", Pearson Education, New Delhi, 2004.

[3] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, " A Survey of Secure Mobile Ad Hoc Routing Protocols", 1553-877X/08/IEEE 2008.

[4] Amit Goel and A.K. Sharma, "Security Trends in Wireless Lan".

[5] Amit Goel and A.K.Sharma, "Secure Communication in Mobile Ad Hoc Network".

[6] Dr. Sanjeev Sofat, Prof. Divya bansal and Rajinder Kumar, "Security in Mobile Ad Hoc Networks", COIT-2008 March 29.

[7] Nishu Garg and R.P. Mahapatra, "MANET Security Issues", *IJCSNS*, **9**, Aug. 2009.

[8] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad Hoc Network".

[9] B. Awerbuch et al, "An On-Demand Secure Routing Resilient to Byzantine Failures", *Wireless Security*, Sept. 2002.

[10] S. Corson and J.Macker, "Mobile Ad Hoc Networking Routing Protocol Performance Issues and Evaluation Considerations", RFC2501, Jan. 1999.

[11] Zhou, L and Haas Z. J., "Securing Ad Hoc Networks" *IEEE Network Magazine*, **13(6)**,1999, pp. 24-30.

[12] Molva, R and Mchiardi, P, "Security in Ad Hoc Networks", PWC 2003, Italy, Sept. 2003.

[13] S.Buchegger and J.L. Boudec, "Performance Analysis of the Confident Protocol in Dynamic Ad Hoc Networks IEEE/ACM Symp.", 2002.

[14] D.A. Maltz, "Resourses Management in Multi-hop ad Hoc Network", CMU-CS-00-150, Nov. 21, 1999.

[15] Po-Wah Yau and chris J. Mitchell , " Security Vulnerabilities in Ad Hoc Networks", *Information Security Group Royal Holloway*, University of London, TW20 0EX, UK.

[16] Ilyas, M., "The Handbook of Ad Hoc wireless Network, CRC Press, 2003.

[17] Danesh, A. and Inkpen K., "Collaborating on Ad Hoc Wireless Network", at www.parc.xerox.com/sl/projects/ubicomp-workshop/positionpapers/danessh.pdf.

[18] Aura T. and maki, S, "Towards a Survivable Security Architecture for Ad-hoc Network", Springer-Vverlag, 2001.

[19] Hoeper , K. and Gong, "Models of Authentication in Ad Hoc Networks and their Related Network Proreties" CACR2004-20003.