Review of Emerging Threats, Vulnerabilities and Techniques of Security on Mobile Ad hoc Networks

Mukesh Azad[1], Rohit Pal[2], Jyoti Nautiyal[1], Mukesh Panday[2], Kuldeep Kumar[2]
[1]M.Tech Student, Uttarakhand Technical University Dehradun(U.K)
[2]M.Tech Student, Graphic Era University Dehradun(U.K)
{doon.azad, errohitpal, jyoti51289, ermukeshpanday1985, kuldeep.geit}@gmail.com

***Abstract*— This article presents a review of various issues on security of Ad hoc networks (AHN) are wireless multi-hop packet networks without any fixed infrastructure. An AHN network is formed solely by its terminals so that each terminal connected to the network provides also relaying service for others i.e. acts as a router. Advantages of such system are rapid deployment, robustness, flexibility and inherent support for mobility. The wireless medium is openly accessible, less reliable and has no obvious physical boundary. An attacker does not need to break any physical barriers to gain access to the wireless medium and can enter the network from anywhere and from all directions. In addition, more complications in security establishment come from the dynamically changing topology, the reliance on node collaboration for network connectivity, the lack-of-trust infrastructure and the lack of a clear line of defense. Since ad hoc networks are built without a fixed infrastructure and centralized management, the protection mechanisms used in tethered networks cannot be adopted directly in wireless ad hoc and sensor networks. External as well as internal attacks on ad hoc network routing protocols disrupt performance of networks and reliability due to the nature of the network. We take a scenario of attacks and vulnerabilities present in the network and discuss the techniques to resolve the problems due to security breached and also about the comparison between the solutions and parameters of ad hoc network show the performance according to secure protocols. We discuss in this paper routing protocol and challenges and also discuss authentication in ad hoc network.**

Keywords-Wireless Network, Ad hoc Network, Security Service, Routing Protocols, Routing Authentication, Hash function and Secure Routing Protocols, Attacks, Secure Routing Protocol

I. INTRODUCTION

Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily [3]. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system [1]. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible Technology for establishing communications in situations which demand a fully decentralized Network without any fixed base stations, such as battlefields, military applications, and other Emergency and disaster situations Since, all nodes are mobile, the network topology of a MANET is generally dynamic and may change frequently.

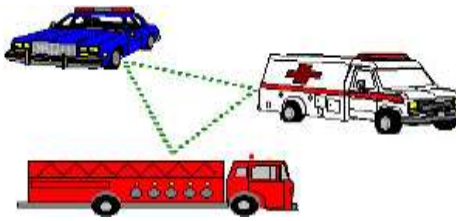

Figure 1. Ad hoc network in emergency

Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, direct *single-hop* transmissions between two hosts can require significant power, causing interference with other such transmissions.

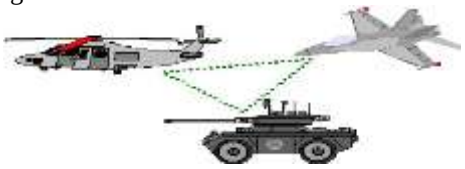

Figure 2. Ad hoc network in war

A router should provide a mechanism to filter out obviously invalid routes. Routers must not by default redistributes routing data they do not themselves use, trust or otherwise consider valid. Routers must be at least a little paranoid about accepting routing data from anyone, and must be especially careful when they distribute routing information provided to them by another party [2].

Figure 1 and Figure 2 shows three nodes where ad hoc network where every node is connected to wireless, and work as access point to forward and receive data. The hierarchy of security is shown in Figure 3, describes the basic model of the security.

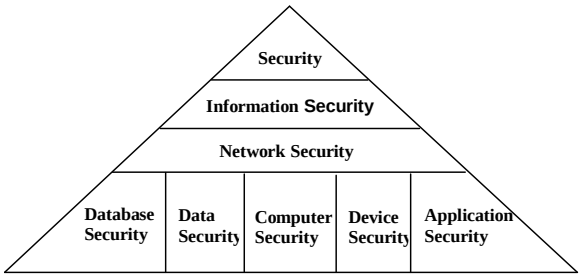

Figure 3. Hierarchy of Security Specializations [17]

Some important keywords we have to explain before going on depth of security on Ad hoc network:

Security: Protection of information and property from theft, corruption or natural disaster, while allowing the information and property remain accessible and productive to its intended user [4].

- *Asset:* "What is to be protected?"
- *Risks:* "What are the threat vectors vulnerabilities and risks?"Risks are the cost of a threat successfully exploiting vulnerability.
- *Protection:* "How will asset be protected?"
- *Tools:* "What will be done to ensure the protection?"
- *Priorities:* "In what order will the protection steps be implemented?"
- *Security mechanism:* A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- *Security service:* A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
- *Threat:* A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
- *Attack:* An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
- *Security Attacks:* Any Action that compromises the security of information owned by an organization.
- *Passive Attacks:* Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis [4].
- *Active Attacks:* Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
- *External attack:* An attack that is caused by a node that does not belong to the network. These are typically active attacks that may lead to the transmission of false routing information, generation of routing loops, partitioning of the network and congestion.
- *Internal attacks:* Attacks are from nodes belonging to the network and are primarily due to being compromised or captured. Internal attacks are more severe attacks, since the malicious nodes sending incorrect routing traffic are already processed through the security mechanisms imposed by the routing framework [8].
- *Security Policy:* In the core of any security effort and a documented policy lessons confusion and brings forward the important underlying assumptions that must be taken into considering when designing a defense. Security policy is necessary to clearly delineate management's objective for the security program and how control will be utilized to accomplish the objectives [4].
- *Security Strategy:* A security strategy is the definition of all the architecture and policy components that make up a complete plan for defense, deterrence and detection. Strategy in nature is proactive.
- *Security Tactics:* Security Tactics are the day today practices of the individuals and technology assigned to the protection of assets. The nature of Tactics is reactive [17].

- *Threat Vector:* A Threat Vector includes information not only about a particular source of harm but also about where it originates and what path it takes to reach the protected assets [17].
- *Vulnerability:* Vulnerability is an exposure in the infrastructure that can lead to threat becoming realized [4].

II. OVERVIEW OF MANET ROUTING PROTOCOLS

Routing Protocols

The Figure 4 shows classification of MANET routing protocols. Forwarding consists of taking a packet, looking at its destination address, consulting a table, and sending the packet in a direction determined by that table. Routing is the process by which forwarding tables are built. Forwarding is a relatively simple and well-defined process performed locally at a node, whereas routing depends on complex distributed algorithms that have continued to evolve throughout the history of networking [8].

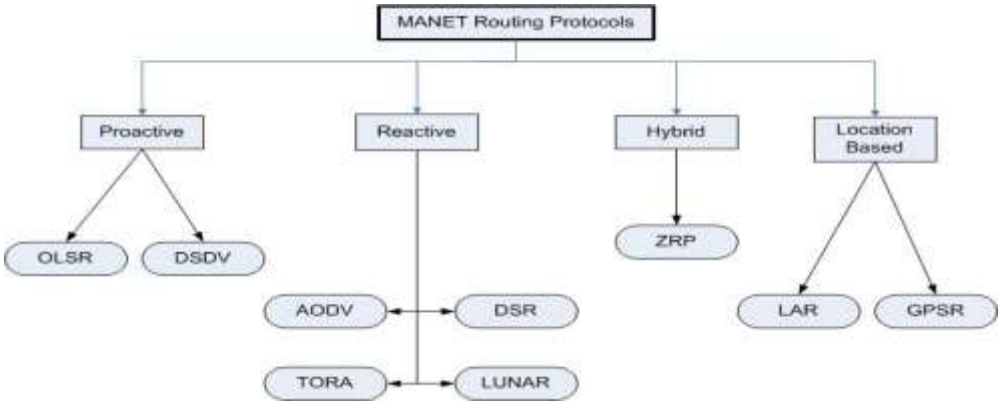

Figure 4. Classification of MANET Routing Protocols

a) Proactive Routing Protocol

A Proactive (Table-driven) Routing Protocol attempts to allow each node using it to always maintain an up-to-date route to each possible destination in the networks, the protocol periodically exchanges routing information with other nodes in order to allow new route to be discovered and existing route to be modified if they break due to factors such as node mobility and environmental changes.

b) Reactive Routing Protocol

A Reactive (On Demand) Routing Protocol only attempts to a discover a route to some destination when it has a packet to route to some destination when it has a packet route to that destination and does not already know a route there; the protocol catches known routes and uses a flooding based discovery protocol when a needed route is not found in the cache [20].

III. SECURITY ATTACK & CHALLENGES

We have to consider external as well as internal attack on MANET. The nature of wireless ad hoc networks makes them very vulnerable to attack. First of all, the mobile nodes are independent and their movements are not controlled by the system, so they can easily be captured, compromised and hijacked. Secondly, since in wireless networks there are no physical obstacles for the adversary, attacks can come from all directions and target any node. Third, in wireless ad hoc networks adversaries can exploit the decentralized management for new types of attack designed to break the cooperative algorithms. Thus following are the ways by which security can be breached [5]:

- *Location Disclosure*

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network [9].

- *Black Hole*

In a black hole attack a malicious node injects false route replies to the route requests it receives, broadcasting itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in

order to perform a denial of service attack by dropping the received packets. [18]

- *Replay*

An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

- *Wormhole*

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes [14].

- *Blackmail*

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [21].

- *Denial of Service*

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture.. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

- *Routing Table Poisoning*

Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

- *Rushing Attack*

Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as ARAN, SAODV, are unable to discover routes longer than two hops when subject to this attack [23]. Developing Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

Breaking the neighbor relationship: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session [19].

- *Masquerading*

During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS [21].

- *Passive Listening and traffic analysis*

The intruder could passively gather exposed routing information. Such a attack can not affect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol [22].

- *Sinkhole attacks:*

In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-

quality route by transmitting with enough power to reach a wide area of the network [10].

- *The Sybil attack:*

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things, including position of nodes, signal strengths, making up nodes that do not exist. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has compromised [13].

- *Selective Forwarding attack:*

It is a situation when certain nodes do not forward many of the messages they receive. The networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.

- *Hello flood attacks*

The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent . All messages now need to be routed multi-hop to this parent, which increases delay [15].

TABLE I CLASSIFICATION OF ATTACK [16]

Attacks	Layers involved	Defenses
Denial of Service	Physical, Link, Network, Transport layers	Priority messages, hiding, monitoring, authorization, redundancy, encryption
Wormhole attack	Link layer, Network layer	proactive Routing protocol, suspicious node detection
Sybil attack	Network layer, Application layer	Identity certificates
Hello flood attack	Network layer	Suspicious node detection by signal strength
Sink hole attack	Link layer, Network layer	Detection on Min Route

IV. SECURITY SOLUTIONS FOR MANET

In a secure wireless ad hoc sensor network, a node is authorized by the network and only authorized nodes are allowed to access the network resources. The generic process to establish such a network consists of bootstrapping, pre-authentication, network security association establishment, authentication, and behavior monitoring and security association revocation. Among these, authentication is of the utmost importance and is an essential service in network security. Other basic security services like confidentiality, integrity and non-repudiation depend on authentication. The main requirements of a routing protocol are quick convergence, scalability, consistency, robustness etc. Additionally to provide extra security guarantees, the routing protocol should also provide, amongst other things, Data Integrity, Origin Authenticity, Non-Repudiation, Timeliness and Ordering. Various solutions have been proposed in literature to deal with many of these security problems. All the schemes can be broadly categorized into the following three groups based on their functionality.

- *Routing Information Techniques*

In these techniques, digital signatures are used to provide Origin authenticity and to an extent data integrity also by having the sender signs the routing messages. This can protect against modified or fabricated routing messages and enables attack detection due to subverted links but not due to subverted routers themselves.

- *Intrusion Detection Techniques*

These techniques are used to detect anomalous behavior in the routers, assuming that intrusion detection devices are available in the network. But the problems associated with these schemes are precise characterization of what exactly constitutes anomalous behavior, as subtle changes made over time could possibly bypass these filters. Also these mechanisms only help in identifying the anomalous behavior but cannot avoid the attack from taking place, making routing table poisoning unavoidable [7].

- *Routing Protocol Techniques*

Several changes have been proposed to the routing protocols and Messaging formats to provide additional security benefits. These methods help in preventing looping, malicious distance vector updates cannot be detected using these techniques. Sequence Numbers are used in along with the routing messages to protect against replay attacks and also to provide orderliness and detection of lost routing messages. But it does not provide any other security guarantees.

V. TECHNIQUES FOR MANET SECURITY

The following are the approaches used for providing security in MANET –

- *Hash Message Authentication Code (HMAC)*

HMAC is designed such that it can use any other available hash function, such as MD5 or SHA-1. The design objectives of HMAC are as follows:

- To use any available hash function;
- To replace the used hash function easily;
- To introduce negligible overhead in addition to the overhead by the used hash function;
- To present a clear cryptographic analysis of the authentication strength.

In the HMAC structure, the key is first padded with zeros on the left such that it becomes b bits long. The padded key K+ is then applied via a XOR operation to ipad, which is 00110110 repeated b/8 times. The result is appended to the message. This makes the input for a selected hash function. In the second round, K+ is applied via a XOR operation to another constant opad, which is 01011100 repeated b/8 times, and appended to the result of the first round. This final bit stream has the hash function applied one more time, which produces an m-bit long MAC. This provides both integrity and authentication.

- *Hash Chain*

A hash chain is generated by repeatedly applying a hash function *h* to a string *M*. In Figure, a hash chain of length three is shown.

$X_2 = h(M)$
$X_1 = h(h(M)) = h_2(M)$
$X_0 = h(h(h(M))) = h_3(M)$

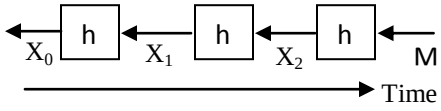

Fig3.0. A hash chain of length 3

The sender may use this hash chain in reverse order for authentication. A receiver initially stores X_0. At a later time, the sender may disclose X_1 and the receiver can verify X_1 by checking $h(X_1) = X_0$. Similarly, the following packages can be verified by releasing the later hash values in the chain [24].

Every router in the network creates a pair-wise mutually exclusive shared key with each of its one-hop and two-hop neighbors, i.e. with every router in all the groups where it is the sender.

This approach is used by TESLA for the authentication of broadcast or multicast messages. In TESLA, a one-way key chain is used to provide authentication. A one-way key chain is generated by repeatedly using the same one-way hash function on an initial key.

- *Bootstrapping (booting)*

It is the phase in which the nodes in a network are made aware of the presence of all or some of the others in the network. During the bootstrapping process, all nodes that want to join the network must gain their identifying credential to prove their eligibility to access the protected network. The identifying credential takes the form of either something that they should have or something that they should know. In the bootstrapping phase the nodes in a network become aware of the presence of the other nodes in their vicinity or in the overall network. Wireless ad hoc networks introduce new challenges for this phase. An important characteristic of wireless ad hoc networks is the lack of centralized security infrastructure. To protect the security of a network, the first step is to build a security infrastructure between the nodes during the bootstrapping phase. The trust infrastructure should satisfy the requirements that only legitimate nodes can join the network; new nodes that may join the network can form a secure association with the nodes already in the network; the trust infrastructure can be set up without the knowledge of the network topology; the credential verification scheme should be strong enough to resist DoS attacks and at the same time should not require large computational ability and memory. In practice, in wireless ad hoc networks, the topology of the network changes quickly and therefore it is difficult to get either a trusted prior context or a trusted third party. For ad hoc networks, it is more natural to self-organize the trust infrastructure since this involves no special nodes, no infrastructure, no centralized configuration point and no shared prior context.

However, an out-of-band authenticated communication channel is often needed in many proposed protocols. For example, in Balfanz *et al.* (2002) a privileged side channel is used to exchange public information to help the node perform the pre-authentication protocol for bootstrapping secure communication in an ad hoc wireless network. Identity-based security schemes are another approach to achieving this goal. Alternatively, a key can be established with a tamper-proof hardware token provided by users [26].

- *Key Distribution, Exchange and Management*

In an ad hoc network, the trustworthiness of a communicating node is crucial. For secure data exchange, a secure association is often established by setting up shared credentials, e.g. a secret key, between neighboring nodes. To establish the security association, key management protocols, including key distribution and key exchange protocols, have core importance in bootstrapping [27]. After bootstrapping, an ad hoc network is initialized and ready to accept any participant with a valid credential. In other words, the possession of a valid credential becomes proof of the trustworthiness of a

newly joined node. The ideal key management service for ad hoc networks should be simple, formed on the fly, never expose or distribute key material to unauthorized nodes, ensure that system security does not succumb to (a few) compromised nodes, easily allow rekeying / key updates, enable withdrawal of keys when nodes are compromised or keys for other reasons should be revocable, be robust to Byzantine behavior and faulty nodes, scale well enough to handle the expected network sizes and node densities and efficiently manage network splits and joins. Signed routing information requires a security association that allows one-to-many signing and verification. Routing messages are often broadcast, and all receiving nodes should be able to check the validity [24]. Messages such as neighbor-detection messages are not forwarded by other nodes. Other routing messages, such as topology information messages in proactive routing protocols and route requests and route replies in reactive routing protocols, are flooded into the entire network. The receiving nodes may not be known to the transmitting node. In addition, bandwidth is limited. Unique signatures for each receiver scale badly. In other words, pair wise keys provide no good option for protection of routing information.

- *SKiMPy*

SKiMPy (Puzar et al., 2005) was designed for MANETs. It seeks to establish a MANET-wide symmetric key for protection of network layer routing information or application layer user data. On MANET initialization, all nodes generate a random symmetric key and advertise it within one-hop neighborhoods through 'Hello' messages. The best key, i.e. the one with the lowest ID number, freshest timestamp or other, is chosen as the local group key [28]. The best key is transferred to the nodes with worse keys through a secure channel established with the aid of pre-distributed certificates. The procedure is repeated until the 'best' key has been shared with all nodes in the MANET.

- *Intrusion Detection*

Wireless ad hoc networking is associated with vulnerable characteristics such as open-air transmission and self-organizing without a fixed infrastructure or centralized management. Consequently, ad hoc networks are more susceptible to attack, and the security challenges in them are more complicated. As the first line of defense, intrusion-prevention techniques, such as encryption and authentication, can be used to defend against intruders. However, even in a fixed-wire network, proactive defense alone is not sufficient to secure a system from all penetrations. A second line of defense system is needed to detect an ongoing attack in the network. If such detection is available, damage may be minimized. An intrusion-detection system (IDS) monitors activities in a system and then analyzes the audit data to determine whether there is a violation of the security rules. An alert is given if a violation known to be malicious is found. Responses to the attack may also be initiated by the IDS accordingly. The available techniques include abnormality, misuse and specification based detection (Mishra et al., 2004) [7].

- *Techniques Against Wormhole Attacks*

Wormholes are difficult to detect because an adversary passes the packets to a distant point from the point at which they are received by using a single hop out-of-band channel. This channel cannot be listened to by the network. Moreover, the real copy of the packet reaches the point that receives the replayed copy later than the replayed copy. Therefore, the replayed copy is fresher than the real copy. Detection mechanisms against wormhole attacks can be based on temporal and spatial analysis of the packets. Geographical and temporal packet leashes introduced in Hu et al. (2003) follow this approach. A geographical leash scheme assumes that nodes are loosely synchronized and location aware.

Temporal leashes use only the transmission and reception times of the packets for detecting wormholes. Temporal leashes require tight time synchronization. Attackers can also adapt to directional antennae by replaying the packets in the same sector as that in which they are received. However, the capabilities of attackers are reduced even with this simplest form of the approach.[14]

- *Techniques Against Sybil Attacks*

To defend against sybil attacks, the identities of every node should be verified. This can be done either directly or indirectly. In direct validation a node directly verifies whether the identity of a neighboring node is valid. For example, a node may assign each of its neighbors a separate channel to communicate and ask them to transmit during a period. Then it checks these channels in a random order within that period. If a node is transmitting in its assigned channel, the node is a physical node. If no transmission is detected on a channel, it indicates that the node assigned to that channel may not be a physical node (Newsome et al., 2004). In indirect validation another trusted node provides the verification for the identity of the node. When two nodes need to establish a link between them, they verify each other's identity through the base station by using these keys (Karlof and Wagner, 2003). At the same time they can be assigned a session key.

Nodes can also be allowed to establish links with a limited number of neighboring nodes. Thus, compromised nodes can only communicate with a limited number of verified neighboring nodes, which also limits the impact of sybil attacks. Random keys assigned to nodes also provide security against sybil attacks. Since a limited number of keys is available to each node, nodes do not have enough keys to generate multiple identities (Newsome et al., 2004) [13].

- *Sinkhole attacks prevention*

Such attacks are very difficult to defend against. One class of protocols resistant to these attacks is geographic routing protocols. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station [11].

- *Hello flood attacks prevention*

This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop [15].

- *Techniques Against Selective Forwarding*

Preventing wormholes, sink holes and sybil attacks cannot guarantee to mitigate black hole and selective forwarding attacks. A compromised node can still act as a black hole or drop selected packets. There are two approaches to defending against selective forwarding: detecting the nodes that selectively forward and developing routing schemes that are more resilient and can deliver packets even when there is a selective forwarding attack. One approach to detecting the nodes that selectively forward is based on acknowledgements (Yu and Xiao, 2006). Every intermediate node that forwards a packet waits for an acknowledgement from the next hop. If the next hop node does not return the same number of acknowledgements as the number of packets sent, the node generates an alarm about the next hop node. However, compromised nodes can also generate acknowledgements for the packets that they dropped, which make this scheme fail. Moreover, a malicious node can generate fake alarms to organize a Denial of Service attack. Authentication schemes and encryption can be used to prevent these kinds of malicious behavior (Yu and Xiao, 2006). Link layer acknowledgements can also be complemented by end-to-end reliability schemes. Multipath routing can be an effective way to mitigate selective forwarding and black hole attacks (Karlof and Wagner, 2003). This requires at least link-disjoint paths, where two paths may share some nodes but no link. Of course, node-disjoint paths, where two paths do not have any node in common, are better and reduce the risk of selective forwarding attack compared to link-disjoint paths. However, disjoint paths are not always available, and when paths are not disjoint, if the selectively forwarding node is the node common to all the paths, then the attack can become as effective as in single-path routing [12].

VI. COMPARISONS OF SECURE PROTOCOLS

At the end of article we provide the comparison of different secure routing protocols of ad hoc network using Table 1.0. Comparison shows which protocol is better in different type of attacks. For example replay attack cover by ARAN but it is not coverable by RAP [2].

TABLE II DEFENSE AGAINST ATTACK [2]

Attack	**Protocol**							
	ARAN	***SRP***	***SEAD***	***ARIADEAN***	***SAODV***	***SLSP***	***OSRP***	***RAP***
Location-Disclosure	No	No	No	No	No	No	No	No
Black- Hole	No	No	No	No	No	No	Yes	No
Replay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Worm-hole	No	No	No	No	No	No	No	No
Black-mail	NA	NA	NA	NA	NA	NA	NA	NA
Denial of services	No	Yes	Yes	Yes	No	Yes	No	No
Routing table-poisoning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Rushing attacks	Yes	No	Yes	Yes	No	No	No	Yes

VII. CONCLUSION

Mobile ad hoc networks present different threats and vulnerabilities due to their nature of openness and its various properties. These properties bring in various different security risks from conventional wired networks, and each of them affects and gives a challenge that how security is provided and maintained. All types of threats identified above give rise to different security requirements, several of which apply to ad hoc routing.

Any protocols and simulations to test them should include the capability to handle each type of node and attack. In this paper, an attempt is made to discuss various attacks and vulnerabilities that exist in ad hoc networks with their techniques and solutions that how the security can be provided without hampering the performance of the network.

VIII. FUTURE WORK

It is demand of time that we have to implement secure reliable as well as efficient routing protocol which is capable enough to provide QOS without compromising security as well as high availability. We are more concern about enhancement of security in AODV. In future we simulate various cases with the help of NS2 and try to overcome possible threats.

Acknowledgment

We have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them. We are highly indebted to UTU faculty members for their guidance and constant supervision as well as for providing necessary information regarding the paper & also for their support in completing the paper. We would like to express our special gratitude and thanks to industry persons for giving us such attention and time. Our thanks and appreciations also go to our friends in preparing the paper and people who have willingly helped us out with their abilities.

REFERENCES

[1] Yih-chun hu, adrian perrig, "A Survey of Secure Wireless ad hoc routing," IEEE security & privacy May-June 2004

[2] Karan Singh, Rama Shankar Yadav, Ranvijay, "A Review Paper On Ad hoc Network Security," International Journal of Computer Science and Security, Volume (1): Issue (1)

[3] Lidong Zhou , Zygmunt J. Haas, "Securing Ad Hoc Networks," Cornell University Ithaca, NY 14853

[4] William Stallings, *Cryptography and Network Security Principles and Practices*, 4th Ed

[5] Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks," IEEE 2004.

[6] Zhou, Z.J. Haas, "Securing ad hoc networks," IEEE NetworkMag. 13 (November/December 1999) 24–30.

[7] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks," in: SixthInternational Conference on Mobile Computing and Networking (MOBICOM'00), August 2000,pp. 275–283.

[8] Lakshmi Venkatraman and Dharma P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," Journal of Parallel and Distributed Computing - Special issue on Routing in mobile and wireless ad hoc networks, Volume 63 Issue 2, February 2003, Pages 214 - 227

[9] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, IETF Network Working Group, January 1999.

[10] E. C. H. Ngai, J. Liu, and M. R. Lyu. "On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC 06), Istanbul, Turkey, June 2006.

[11] M. Zorzi and R.R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Trans. Mobile Computing, vol. 2, no. 4, Oct.-Dec. 2003.

[12] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communications Review (MC2R) Volume 1, (2002).

[13] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS'02).

[14] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05).

[15] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM, 47(6):53-57.

[16] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[17] Roberta, Bragg, Mark, Rhodes-Ousley, Keith Strassberg, *The Complete Reference Network Security*

[18] E. A. Mary Anita and V. Vasudevan, "Black Hole attack on multicast routing protocols," JCIT, Vol.4, No.2, pp. 64–68, 2009.

[19] Y. C. Hu, A. Perrig and D. B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol"; Proceedings of ACM WiSe2003, Sep, 2003.

[20] G.Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing:A Routing Scheme for Ad Hoc Wireless Networks", in Proceedings of ICC 2000, New Orleans, LA, Jun. 2000.

[21] Y. Xiao, X. Shen, and D. -Z. Du (Eds.), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer, 2006

[22] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, pp. 38-47, 2004.

[23] SanzgiriK, DahillB, Levine B.N and Belding-Royer E.M, "A secure routing protocol for Ad-hoc networks," Proc. Of IEEE ICNP, 2002

[24] Erdal Çayırcı, Chunming Rong, *Security in Wireless Ad Hoc and Sensor Networks*, Willy, 2009

[25] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.

[26] R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks," Proc. IEEE GLOBECOM, San Francisco, CA, Dec. 2003, pp.1511-1515.

[27] Jukka Valkonen, Key Management in Ad-Hoc Networks, Helsinki University of Technology, Laboratory for Theoretical Computes Science

[28] Matija Pužar, Jon Andersson, Thomas Plagemann, Yves Roudier, "SKiMPy: A Simple Key Management Protocol for MANETs in Emergency and Rescue Operations", University of Oslo, February 2005

[29] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Commun. Surveys and Tutorials, vol. 19, no. 4, pp.78-93, 2008.

[30] Zhou L. and Haas Z.J, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, 1999