ISSN No. 2278-3091

Volume 1, No.3, July – August 2012

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://warse.org/pdfs/ijatcse05132012.pdf

A Study on the Security and Routing Protocols for Ad-Hoc network

Mrs. Sneha Kumari[1], Dr. Maneesh Shrivastava[2]

[1]Department of Information Technology, LNCT, Bhopal, India, sneha3024@gmail.com

[2]Department of Information Technology, LNCT, Bhopal, India, maneesh.shreevastava@yahoo.com

ABSTRACT

The Ad Hoc network does not rely on a preexisting infrastructure also it lacks a centralized administration. The decentralized architecture makes ad hoc network much vulnerable to various attacks. In this paper we analyze the major vulnerabilities in the MANET along with the various attack types taking place within it. Then we present a review over current solution and the various routing protocols emphasizing over the security issues of the ad hoc network.

Key words: Ad-Hoc, attacks, MANET, routing protocol, security, vulnerability.

1. INTRODUCTION

A Mobile ad-hoc network (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. *ad hoc* is a Latin word which means "for this purpose”. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the large internet [8].

As ad hoc networks do not have any fixed infrastructure, all network functions can be performed by the mobile nodes themselves in a self-organizing manner. This gives rise to much vulnerability in ad hoc networks, making the issue of security very important and challenging [1]..

The mobile ad hoc network has the following typical features:-

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

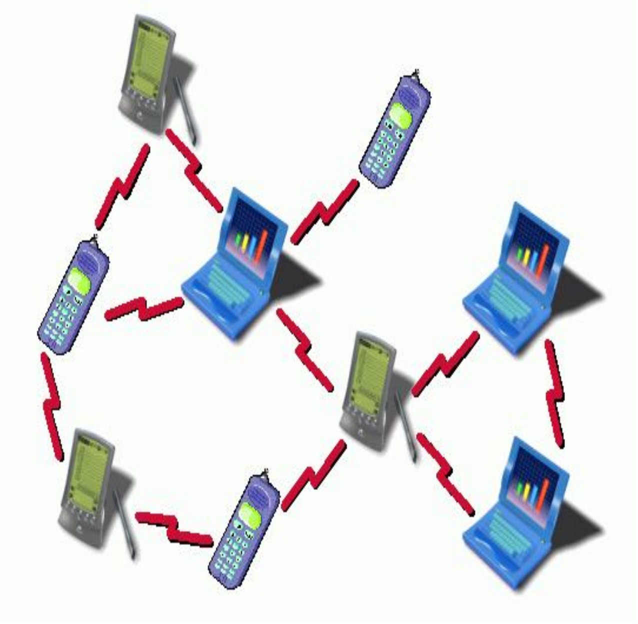


Figure 1: A Basic diagram showing an Ad hoc network

Figure1 given above shows the generic architecture of an Ad hoc network [12] .The network consists of various nodes interacting with each other. All of these devices are movable and hence forming decentralized Ad hoc network architecture.

2. VULNEREBILITY IN AD HOC NETWORK

Mobile ad hoc network is insecure by its nature: there is no such a clear line of defence because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviours that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the security of it [4].

The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons:

a) The wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering.

b) The lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms.

c) Mobile devices tend to have limited power consumption and computation capabilities which make it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms

d) In MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with

e) Node mobility enforces frequent networking. Reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between state routing information and faked routing information [3].

3. SECURITY IN AD HOC NETWORK

Security is the most often cited concern with wireless networks. Wireless networks pose unique security problems. Power and computation constraints are often higher in wireless networks, making security requirements different.

Providing adequate security measures for ad hoc networks is a challenging task. In a security concept, typically striving for goals like authenticity, integrity, confidentiality, non-repudiation and availability, authentication of communicating entities

Authentication means that correct identity is known to communicating partner.

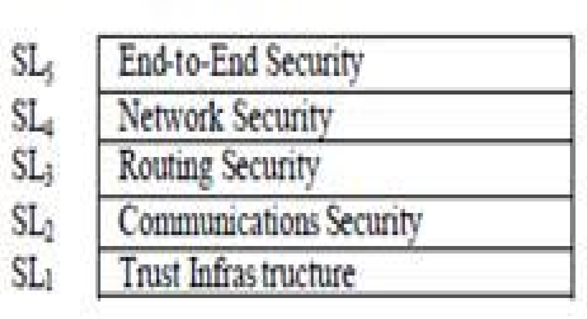
Confidentiality means certain message Information is kept secure from unauthorized party.

Integrity means message is unaltered during the communication.

Non-repudiation means the origin of a message cannot deny having sent the message.

Availability means the normal service provision in face of all kinds of attacks [7][11].

Figure 2 shown below depicts five-layer security architecture for MANETs, and the functionalities of each layer are illustrated as below:



SL_5	End-to-End Security
SL_4	Network Security
SL_3	Routing Security
SL_2	Communications Security
SL_1	Trust Infras tructure

Figure 2: Security Architecture for MANET

A. SL1, Trust Infrastructure Layer: refers to the basic trust relationship between nodes.

B. SL2, Communications Security Layer: refers to the security mechanisms applied in transmitting data frames in a node-to-node manner.

C. SL3, Routing Security Layer: refers to security mechanisms applied to routing protocols.

D. SL4, Network Security Layer: refers to the security mechanisms used by the network protocols which perform sub-network access operations from end system to end system.

E. SL5, End-to-End Security Layer: refers to end system security, such as SSL, SSH, and any application-specific security protocol [3] [5] [9].

3.1 Security Attack Types

Although there are numerous types of attack in MANET but we can categorize them in two primary attack types as:

- Internal Attacks: - Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes.

- External Attacks: - External attacks are attacks launched by adversaries who are not initially authorized to participate in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations.[10]

Besides these primary attacks the Ad hoc network may suffer from some of the following active attacks:-

A. ***Impersonation or Spoofing:*** In this type of attack one Entity assumes the identity and privileges of another Entity without restrictions and without any indication visible to the recipients of the impersonator's calls that delicately has taken place[3].

B. ***Wormhole attacks:*** A compromised node in the ad hoc networks collides with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations [13].

C. ***Black-hole Attack:*** The purpose of this attack is to increase the congestion in network. In this attack the malicious node does not forward any packets forwarded to it, instead drops them all. Due to this attack the packets forwarded by the nodes do not reach their intended destination and the congestion in the network escalates due to retransmissions [14].

D. ***Grayhole attacks:*** A Grayhole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes. In this type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. This type of attacks is more difficult compared to black hole attack[3].

E. ***Eavesdropping:*** The goal of eavesdropping is to steal the confidential data such as the public or private keys, or even passwords of nodes; that must be kept secret during communication. As such data are very confidential they must be secured from unauthorized access.

F. ***Denial of Service (DoS):*** Denial of Service (DoS) is the degradation or prevention of legitimate use of network resources. which aims to crab the availability of certain node or even the services of the entire ad hoc networks. This is carried out by flooding the network traffic usually.

G. ***Attacks Against Routing:*** Attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery . Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path [4].

H. ***Location Disclosure:*** The location disclosure attack intends to target the privacy requirements of the ad-hoc network. In this attack the attacker, by doing traffic analysis or using simple monitoring, approaches and finds the location of the destination node in the network. By knowing the intermediary nodes the attacker can find the node of concern and gain the information about the structure and the topology of the network [14].

3.2 Security Solution to the Ad Hoc Network

The solution to the security problem to the ad hoc network is achieved by applying and taking concern to the security goals such as authenticity, integrity, confidentiality, non-repudiation and availability, authentication of communicating entities.

These security goals can achieved by making use of different techniques such as secured routing protocol, trust evaluation based technique, power awareness, clustering algorithm etc. We will describe the most important technique in this paper which is the secured routing protocol.

4. ROUTING PROTOCOL

Routing is very important issue in Ad hoc networks. Each node in the network must be able to take care of routing of the data and can discover multihop paths.

Ad Hoc Routing Protocols are mainly categorized into three categories which are:

i. i. Unicast: - Unicast delivers a message to a single specific node.

ii.

iii. ii. Multicast: - Multicast delivers a message to a group of nodes that have expressed interest in receiving the message.

iv.

v. iii. Broadcast: - Broadcast delivers a message to all nodes in the network.

We will discuss some of the routing techniques of Unicast method having the subtype Id Based Flat method which again is categorized into three main categories:-

A) **Proactive Protocols**:- this is also known as the table driven Routing protocol. In this method the information is periodically advertised to all nodes to keep the information up to date. Each nodes maintains a routing table which contains info about the other nodes. In this method the route info is accessed always using the routing table entry. Examples of proactive routing are given below:-

- ***DSDV (Destination sequenced distance-vector routing protocol) :*** In this mechanism, routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbours at regular intervals to keep up-to-date view of the network. Neighbours node use missing transmissions to detect broken links in the topology. When a broken link is found, it is assigned a metric value of infinity and the node that detected broken link broadcasted an update packet, to inform others that the link is chosen [2].

- ***R-DSDV*****:** It is an enhancement of DSDV and known as randomized version of Destination Sequenced distance vector. It uses congestion control mechanism using probabilistic model.

- ***LSP (Link State Protocol):*** The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

- ***FSR (Fish State Routing):*** In FSR routing information is disseminated. In this method the node rapidly shares information with its nearest neighbourhoods and less frequently with distant nodes. Thus it alleviates problem of message overhead but it increases bandwidth issue when node density increases. It is a type of LSP [2].

- ***CGSR (Cluster head Gateway Search Routing):*** In this method the mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads.

- ***OLSR (Optimized Link State Routing):*** OLSR is a proactive link-state routing protocol, which uses *hello* and *topology control* (TC) messages to discover and then disseminate link state information throughout the mobile ad-hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

- ***TBRPF (Topology based reverse path forwarding):*** It is based on link state algorithm. It uses tree topology and dijkstra algorithm concepts to minimize overhead and increase robustness. Its Reverse path forwarding process is applicable to large networks which greatly decreases collision and traffic [2].

- ***DREAM (Distance Routing Effect Algorithm for Mobility):*** It follows the concept of directional flooding to forward data packets. Thus there will be multiple copies of each packet at the same time. This increases probability of using the optimal path; however, it decreases its scalability in large scale networks [2].

B) Reactive Protocols: **-** These are also known as the On Demand Routing Protocol. This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.

2. Excessive flooding can lead to network clogging.

Examples of Reactive routing Protocol are given below:-

- ***DSR:*** Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance.

- ***AODV (Ad hoc on demand distance vector routing):*** This protocol [19] is mixture of DSR and DSDV routing protocol. It uses route discovery process same as DSR make use of hop by hop routing like DSDV. It differs with DSR in the way that it does not store the information of entire routing its buffer. And Route maintenance is same as DSDV [2].

- ***FORP (Flow Oriented Routing Protocol):*** The key feature of this protocol is applying a prediction based scheme for selecting and maintaining its routes. It can predict the link expiration time (LET) for a given link- For a complete description about used the prediction algorithm, refer to , and consequently it can predict a route expiration time (RET) for a given path. FORP uses such predictions to select the longest likely to live paths and to handoff the current sessions and find alternative paths before the expiration of the currently used ones

- ***TORA***: TORA builds and maintains a Directed Acyclic Graph rooted at a destination. No two nodes may have the same height. Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally-ordered heights at all times, TORA achieves loop-free multipath routing. The protocol performs three basic functions:

1. Route creation
2. Route maintenance
3. Route erasure

- ***ABR (Associativity based routing protocol):*** The ABR protocol is a source-initiated on-demand routing protocol that consists of the following three phases: (a) route discovery phase, (b) route reconstruction phase, and (c) route deletion phase. It is also known as distributed long lived routing protocol for ad hoc networks.

- ***PLBR (Preferred Link Based Protocol):*** This protocol minimizes control overhead by using subset of preferred list. Selections of this list can be based on degree of node.

- ***SSA (Signal Stability Based Adaptive Routing Protocol):*** It is a variant of the AODV protocol to take advantage of information available at the link level. Both the signal quality of links and link congestion are taken into consideration when finding routes. It is assumed links with strong signals will change state less frequently. By favouring these strong signal links in route discovery, it is hoped routes will survive longer and the number of route discovery operations will be reduced. Link signal strength is measured when the nodes transmit periodic *hello* packets. One important difference of SSA from AODV or DSR is that paths with strong signal links are favoured over optimal paths. While this may make routes longer, it is hoped discovered routes will survive longer.

c) Hybrid Protocols: - Hybrid MANET routing protocols integrate suitable proactive and reactive MANET protocols. The resulting hybrid protocol achieves better performance than its components and is able to adjust dynamically to different network conditions. Hybrid routing protocol combines the advantages of both proactive and reactive protocols. Hybrid MANET routing protocols are lightweight, simple and designed to avoid excessive control overhead.

Example of hybrid protocols are given below:-

- ***ZRP (Zone Routing Protocol) :-*** It is a routing protocol with both a proactive and a reactive routing component. ZRP was proposed to reduce the control overhead of proactive routing protocols and decrease the latency caused by route discovery in reactive routing protocols. ZRP defines a zone around each node consisting of the node's *k*-neighborhood (that is, all nodes within *k* hops of the node).

- ***CEDAR (Core Extraction Distributed Ad hoc Routing Protocol):-*** It supports QoS reliable mechanism and based on extracting core nodes in the network. It employs a distributed algorithm to select core nodes [2].

- ***SRP(Secured Routing Protocol):-*** To meet the requirement of day to day rising ad hoc network demands it is necessary to have a secured protocol which can efficiently deliver the various requirement needs in a secured manner. SRP is a hybrid protocol which combines both the proactive and reactive method in order to get a well secured and effective routing protocol.

Figure 3 and Table 1 given below shows the overall classification and related details of various Ad hoc routing protocol:

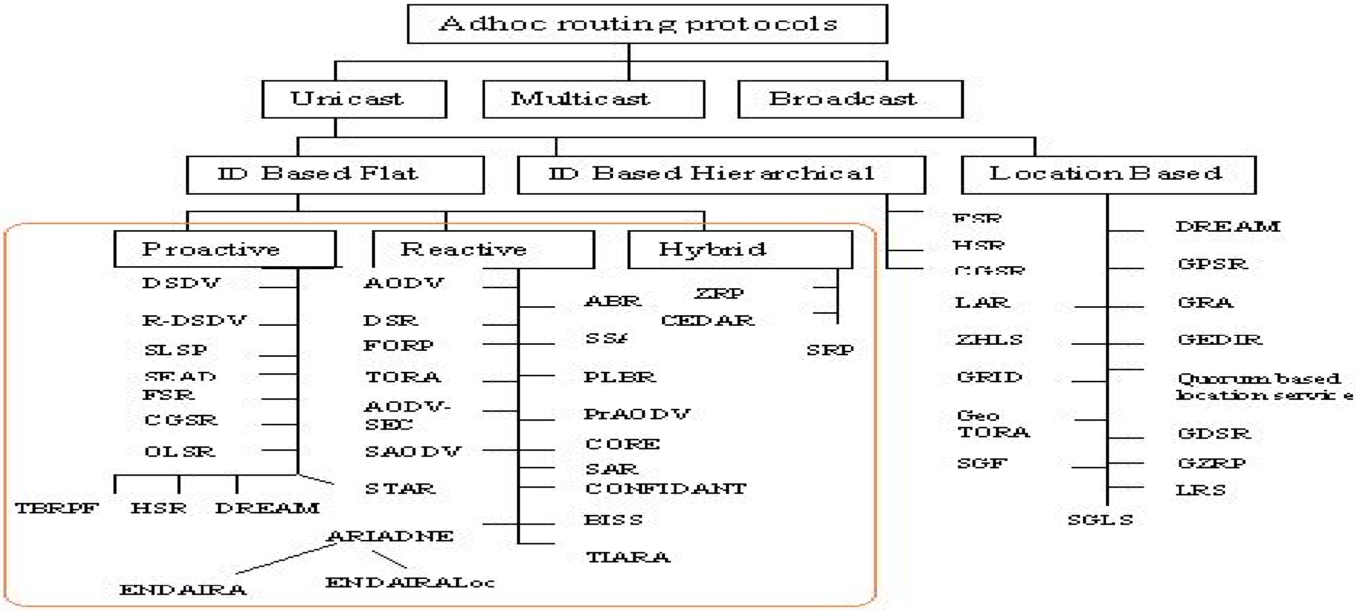


Figure 3: Classification of Routing Protocol

Table 1: Table showing various Secured Routing Protocol

PROTOCOL	CATEGORY AND SUBTYPES	SECURING METHOD OR FUNCTION	SECURES AGAINST
SLSP (Secured Link State Protocol	Proactive and is based on LSP Protocol	TTP	Dos attack and Byzantine adversaries.
2.SEAD (Secure Efficient Ad hoc Distance Vector Routing Protocol)	Proactive and is based on DSDV protocol.	Uses Clock Synchronization method.	DoS attack.
3.SAODV (secured AODV)	Reactive and is based on AODV Protocol.	Online Key Management Scheme	Routing attacks and some spoofing attacks.
4. CONFIDANT (Cooperation of nodes fairness in dynamic ad hoc network)	Reactive based on DSR routing Protocol.	Trust calculation	Source routing protocols *against* adversary nodes and many DOS Attacks.
5. ARAN	Reactive based on DSR routing Protocol	Online Trusted Certification Authority	spoofing, fabrication, modification, DoS and disclosure attacks.
6. ARIADNE	Reactive based on DSR routing Protocol	TESLA	Routing attacks and many types of DoS attacks.
7. Pr AODV	Reactive and based on AODV Protocol.	Mobile gateways	Routing attacks, spoofing attacks ad some DoS attacks.
8. CORE	Reactive based on DSR routing Protocol	Reputation mechanism for monitoring of the cooperativeness of nodes	DoS attacks, spoofing attacks and jamming attacks.
9. ENDAIRA	Reactive based on ARIADNE routing Protocol	Public Key System	active 1-1 attack, Routing attacks and many types of DoS attacks
10. ENDAIRA Loc	Reactive based on ENDAIRA routing Protocol	Symmetric Key Mechanism	man in middle attack as well as wormhole attack
11. SAR	Reactive based on DSR routing Protocol	Key Distribution or secret sharing mechanism	Interruption, interception, modification, fabrication,
12. BISS (Building Secure Routing out of an Incomplete Set of Security Associations)[	Reactive	Provision of Shared Secret Key Mechanism	Routing attacks and many types of DoS attacks including flooding attacks.
13. TIARA	Reactive	Online Public Key Infrastructure	Resource depletion attack, Flow disruption attack, Route hijacking
14. AODVSEC	Reactive and based on AODV Protocols	X.509 Certificate	Routing attacks, spoofing attacks ad some DoS attacks.
15. SPREAD	Hybrid	Threshold Secret Sharing	eavesdropping and colluded attacks
16. SRP	Reactive based on DSR routing Protocol	Existence of a security association between each source and destination	Many of the DoS attacks.

5. CONCLUSION

This paper has presented a study of the Ad Hoc network, Related Security measures and their solution along with the various routing protocol. An attempt is made in order to make a listing of various routing protocol and related techniques. The overall study presents a brief description over MANET and its security measures..

REFERENCES

1. Yao Yu+ and Lincong Zhang. **A Secure Clustering Algorithm in Mobile Ad Hoc Networks**, College of Information Science and Engineering, Northeastern University, IPCSIT, Vol. 29 IACSIT Press, Singapore, 2012.

2. Umang Singh. **SECURE ROUTING PROTOCOLS IN MOBILE ADHOC NETWORKS-A SURVEY AND TAXANOMY**, 1Asstt Prof., Department of Information Technology, I.T.S Management & IT Institute, Ghaziabad (U.P), India, © 2009 - 2011 IJRIC & LLS.

3. Er. Banita Chadha and Er. Zatin Gupta. **Security Architecture for Mobile Adhoc Networks**, IJAEST, Vol No. 9, Issue No. 1, pp. 101 – 104.

4. Wenjia Li and Anupam Joshi. **Security Issues in Mobile Ad Hoc Networks - A Survey**, Department of Computer Science and Electrical Engineering University of Maryland, Baltimore.

5. M. Bechler□, H.-J. Hof†, D. Kraft†, F. Pählke† and L. Wolf□, “**A Cluster-Based Security Architecture for Ad Hoc Networks**”, IEEE INFOCOM ,2004.

6. Asad Amir Pirzada and Chris McDonald. **Establishing Trust In Pure Ad-hoc Networks**, Australian Computer Society, Inc,2004.

7. P. Caballero-Gil. **Security Issues in Vehicular Ad Hoc Networks**, *University of La Laguna ,Spain.*

8. http://en.wikipedia.org/wiki/Mobile_ad-hoc_networks

9. Tim Leinm¨uller+, Elmar Schoch_ and Christian Maih¨ofer+. **Security Requirements and Solution Concepts inVehicular Ad Hoc Networks**, +DaimlerChrysler AG, Group Research and Advanced Engineering, {Tim.Leinmueller|Christian.Maihoefer}@DaimlerChrysler.com University of Ulm, Institute of Media Informatics, Elmar.Schoch@uni-ulm.de.

10. Jean-Pierre Hubaux, Levente Butty´an and Srdan C˘ apkun. **The Quest for Security in Mobile Ad Hoc Networks**, ACM 2001.

11. Frank Stajano and Ross Anderson. **The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks**, Springer-Verlag Berlin Heidelberg 1999.

12. http://www.ustudy.in/node/8252.

13. S. A. Razak, S. M. Furnell and P. J. Brooke. **Attacks against Mobile Ad Hoc Networks Routing Protocols**, Network Research Group, University of Plymouth, Plymouth, Devon PL4 8AA info@network-research-group.org

14. Harshavardhan Kayarkar. **A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques** , M.G.M’s College of Engineering and Technology, Navi Mumbai, India