Implementation of an Enhanced Algorithm for Eliminating the Malicious Nodes in Ad Hoc Networks

[1] POONAM SIHAG
[1]M.Tech Scholar, Computer Science
And Engineering, Om Institute of
Technology and Management,
Juglan (Hisar)

[2] Saurabh Charaya
[2]Assistant Professor & HOD,
Computer Science and Engineering,
Om Institute of Technology and
Management,Juglan(Hisar)

Abstract: The advancement in wireless technologies and the high accessibility of wireless equipment in everyday devices is a factor in the success of infrastructure-less networks. MANETs are becoming more and more common because of their simplicity of organization. Each node is allowed to movement independently on any path and can alter its connections to different nodes. Security is a basic necessity in MANET. The pernicious node in the network act as a ordinary node, so there is a need of security solution to keep from different attacks. An attacker can change the routing protocol and intrude the network activities through mechanisms such as selective forwarding, packet drops, and data fabrication. Security issues in mobile ad hoc network are hidden by different strategies that were presented in past decade. Out of all security issues in MANET, wormhole attack is considered one of the most challenging adversarial modules that tremendously affect the communication system in MANET. A proper security solution is required for networks to ensure both path and data packet delivery operations. . In this paper a systematic survey is done on the current condition of the research results on wormhole attacks. In this paper a qualitative study for eliminating the malicious nodes in ad hoc networks has been done.

1. INTRODUCTION

Mobile Ad hoc Network topology is dynamic that can change quickly on the grounds that the hubs can move openly and compose themselves arbitrarily. This property of the nodes makes the mobile ad hoc network unpredictable from the point of view of scalability and topology. Because of their absence of infrastructure and their capacity to function without the utilization of a central authority or Centralized Controlling devices, Mobile Adhoc Networks are becoming more and more common. These networks are appealing in those locations where it is costly to deploy wired infrastructure e.g. hazardous situations. A Mobile ad hoc network is a collection of portable nodes where nodes are associated to each other based only upon their mutual understanding. They are nodes without settled framework and without centralized administration. These nodes are associated via wireless medium, nodes are independent to move from one place to another and hence topology is also dynamic. Wormholes can either be used to examine the traffic throughout the network or to crash packets selectively or totally to affect the flow of information. The security mechanisms that are used for wired systems such as authentication and encryption are useless under hidden mode of wormhole attack because the nodes do not modify their headers but only forward these packets. But the attack in participating mode is more complicated, because if it once launched, it is difficult to detect.

Security issues in MANETs

There are many security issues that are need to be resolved in Mobile networks, The main issues are:

- The unique characteristics of Mobile ad hoc network present a new set of serious challenges to security design such as peer to peer network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. This allows attacker to infiltrate the network and carry out attack on its participants with the purpose of altering or stealing the information from the network [1].
- A compromised node of the network also have access to encryption keys and authentication information .In many networks, a malicious nodes could falsely route the routing packets into the network or by modifying routing information. Attackers might see an advantage in selectively forwarding packets that pass them [2].
- Among numerous possible threats and attacks like external and internal attacks, active attacks and passive attacks, Mobile network are particularly susceptible to denial of service attacks [3].

Recently, a lot of research has been focused on the cooperation issues in mobile network. Several related issues are briefly presented here [6].

2. *Related Work*

Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP) can be connected as an expansion of Dynamic Source Routing (DSR) protocols [6, 7] .The necessity for SRP protocol is the presence of a Security Associated (SA). It applied security associated only at the end nodes and no need for any cryptographic methods at intermediate nodes. For each route request (as well as reply), SRP used two numbers to identify the request to improve the security; one is a sequence number that is increased periodically. The MAC field is generated by a key hash algorithm, which its input is the entire IP header, the route request packet and the shared key. Two MAC fields are generated by the source for the request packet and by the destination for the reply packet to verify the authentication of packets from the original nodes. SRP ensures the discovery of right network data within the sight of false nodes [7].

Ariadne

Ariadne applies security protocol above on-demand routing protocols for ad hoc networks. It can authenticate routing messages using TESLA. TESLA is an efficient authentication method that achieves an asymmetry protocol from clock synchronization and delayed key disclosure, rather than from computationally. This protocol needs synchronization methods since the authentication is done using clock time. The evaluation for this protocol is done by comparing Ariadne to a version of Dynamic Source Routing protocol (DSR) [18]. Trust-Aware Routing Protocol (TARP) TARP [12] is a new proposed protocol idea (Abusalah.et al., 2006). It is building as part of routing protocol not like another security protocol that would be added as a new layer to the routing protocol. The TARP secures trusted directing that is done by assessing the trust level of its neighbors utilizing properties. These properties are battery power and software configuration. In this protocol when a route path is selected the selection must be not considered only the shortest path factor but also the nodes' power factor (battery power). Most of the protocol focuses on confidence and integrity security requirements, but TARP focuses on security availability (that the network resources are available all the times to keep the connection stable). The performance evaluation of TRAP that applied to DSR shows improvement to the network availability and reduces the routing traffic sent and received [14].

Secure Dynamic MANET On-Demand (SEDYMO) [9]

This protocol is an extension to the reactive protocol DYMO (Dynamic MANET On-demand) (Chakeres and Perkins, 2007). To enforce security to DYMO, hash chain and digital signature is required (Helena and Jordi, 2007). The hash chain is to guarantees the quantity of hops (common field) that the route request traverse isn't adjusted by any unwanted node. To validate the non mutual fields and authentication of the packets a digital signature is used. A distributed Certificate Authority is required to apply certificates to each node. Each intermediates node has to check the signature of the packet is correct and the hash chain for the hopes' number is right. Then the node adds it is signature and increase hope count and hash the hash value after that it can broadcast the packets to next neighbors. For Error message, a signature is added to verify the node that constructs the Error message [14].

Secure Efficient Distance Vector Routing (SEAD) [9]

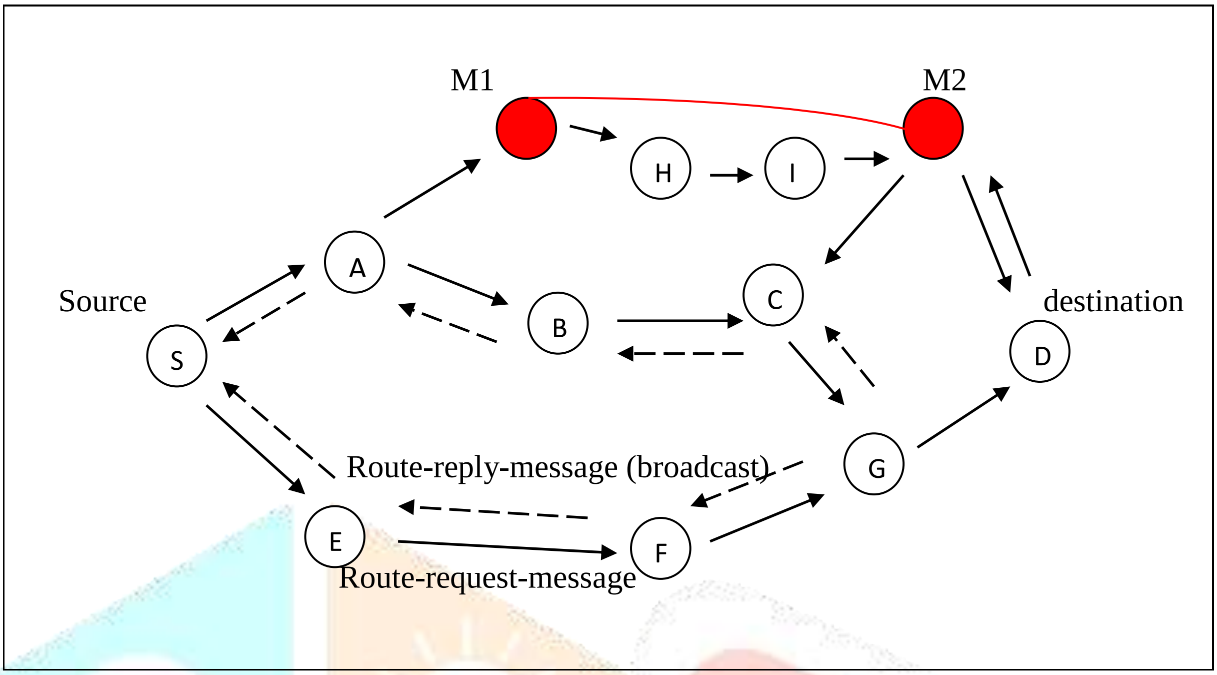
SEAD is a proactive secure routing protocol based on DSDV-SQ-protocol. It does not rely on asymmetric encryption primitive but instead it relies on one-way hash chain for Security. The algorithm expects that there is some verified and secure approach to convey the initial key. This could be done by key delivery in advance or by using public key encryption and signatures for key delivery. The essential thought of SEAD is to verify the sequence number and metric of a routing table update message utilizing hash chains elements. The source of each routing update message in SEAD should be validated since an attacker might have the capacity to create routing loops through the impersonation attack. There are two different approaches proposed such as broadcast authentication mechanism, TESLA and Message Authentication Codes [7, 9].

3. LITERATURE SURVEY

Y.C. Hu, A. Perrig, D.B. Johnson, proposed "Packet leashes in 2003 As mobile ad hoc framework applications are sent, security creates as a primary need. In the wormhole assault, an assailant records packets (or bits) at one area in the framework, passage them (possibly particularly) to another region, and retransmits them there into the framework. It introduce another, general mechanism, called packet leashes, for recognizing and protecting against wormhole attacks, and we exhibit a particular protocol, called TIK, that executes leashes [13].**L.** Hu and D. Evans, Feb. 2004 proposed a conceivable solution to decrease the security dangers is to utilize directional antennas rather than unidirectional ones or in conjunction with them. Because of their complexity, higher expenses and bigger sizes, directional antennas are not generally utilized as a part of remote sensor network, but recent innovation patterns may support this strategy [16]. H.L.Nguyen , U.T .Nguyen, in Apr,2006 Security is an essential in compact especially in delegated frameworks (MANETs). It discusses about how the preparing postponement of honest to goodness hubs the quantity of attackers and their positions impact the execution estimations of a multicast session [17]. Y. Zhang et al., “Location-Based Security Mechanisms for Wireless Sensor Networks,” Feb. 2006 The huge advances of hardware producing technology and the development of effective software algorithm make technically and economically feasible a network made out of various, small, low cost sensors utilizing remote communications, that is, a remote sensor network. WSNs have attracted intensive interest from both academic and industry because of their wide application in civil and military situations. [18]. Sun Choi, proposed WAP, in 2008 the adaptability and transparency of mobile ad hoc networks MANETs make them appealing for different kinds of applications. With a specific end goal to give secure communication in mobile ad hoc networks, it is required to comprehend different attacks at various layers of the communication protocol stack. It provides organized and far reaching investigation of prominent security attacks detailed in the literature for mobile ad hoc networks. Likewise, we additionally examine different well known reactive and proactive security arrangements proposed in literature to protect those attacks in MANETs [6**]. F.Nait-Abdesselam, 2008** an efficient technique is determined to distinguish and avoid wormhole attacks in the OLSR protocol. This strategy first attempts to pinpoint interfaces that may possibly be a part of a wormhole tunnel. At that point a legitimate wormhole detection system is associated with suspicious connections by methods of exchange of encoded probing packets between the two supposed neighbors (endpoints of the wormhole). The proposed solution displays various advantages, non-reliance on any time synchronization or location

4. Proposed Work

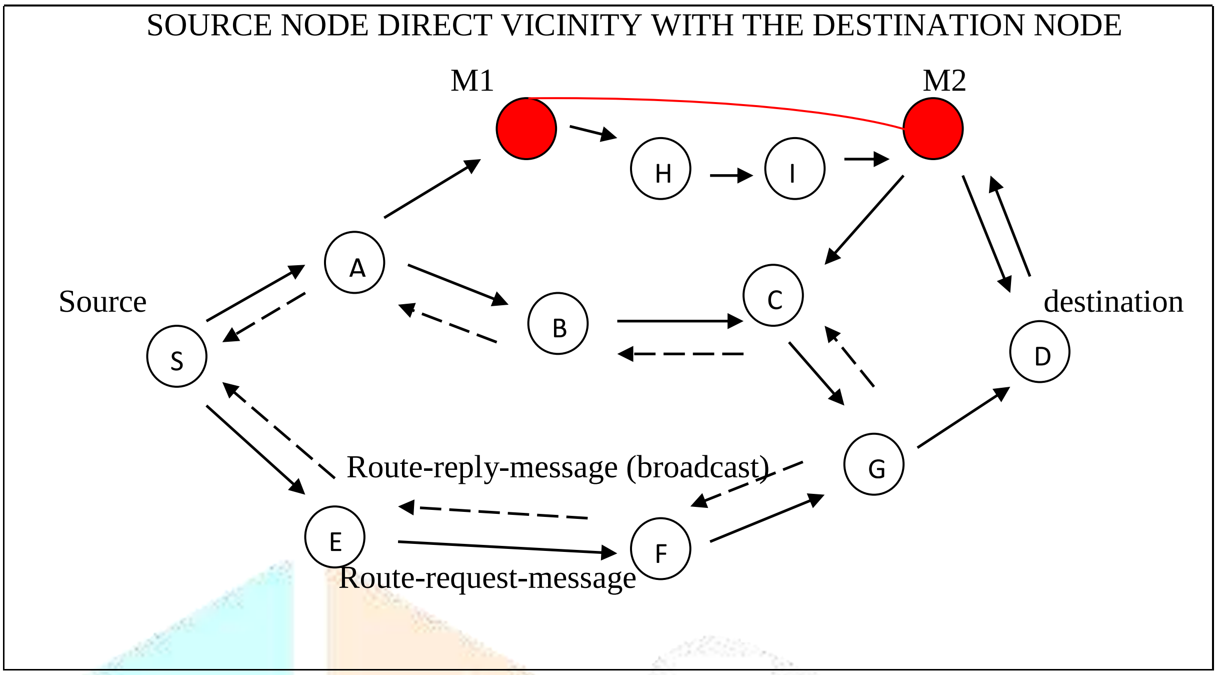
The communication in Mobile Ad hoc network is multi hop communication where source node communicates with destination node utilizing moderate node in order to save the bandwidth and power. The major activity in Ad hoc Network is to find the suitable path in order to delivery of the data packets. The route must be chosen such that all nodes in the path are trustworthy, non malicious, unselfish and minimum hop count. In this technique secure path is discovery from source node to destination node via the intermediate node and detect the inconsistency if malicious nodes are present in Mobile Ad hoc Network.



The source node sends a Route request message to destination node via the intermediate nodes immediately after the deployment of the mobile nodes. Each intermediate node that receives a Route request message checks the Request packet. If the source node is directly in the vicinity of the destination node. The destination node unicast the Route-reply message otherwise destination node broadcast the Route-reply message via the intermediate nodes to the source. The source node selects the shortest path to send the data packet.

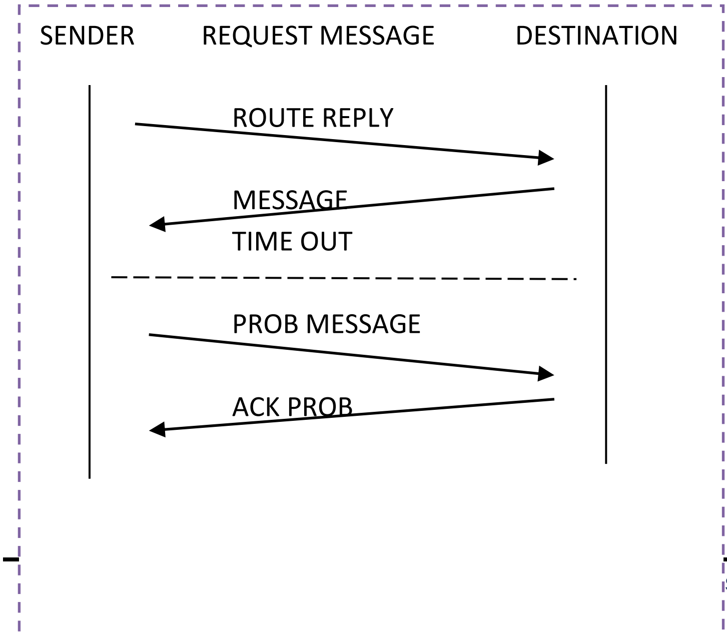
In encapsulation-based Wormhole attacks, intermediate nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. The source node broadcast the Route Request Message to the destination via intermediate nodes. The source node send a Route request message containing following fields source address, source sequence number, broadcast id,, destination address , destination sequence number and hop count.

When the node receives an encrypted Probing packet, first it decrypts that packet and then verifies the sender's identity. If the authentication is successful, the node builds an ACK prob that contains the state of the sender and the large random number that is chosen by the sender. In the same way the node hashes the ACK prob and encrypts it before sending it. After its reception, the sender verifies the validity of the ACK prob message before using the information it contains. Once again, the originator of the Probing packet checks whether the ACK prob arrived within the required timeout. Similar to the Route request and Route reply procedure, the originator also decides in this exchange about possible suspicious links. To choose whether a suspicious connection is navigating a wormhole tunnel, the node looks at its evaluation of the reputation of the other endpoint of the suspicious connection with the


SOURCE NODE DIRECT VICINITY WITH THE DESTINATION NODE
M1
M2
H
I
A
Source
B
C
destination
S
D
Route-reply-message (broadcast)
G
E
F
Route-request-message

other node's evaluation of its own reputation status. If the result of the reputation of the remote node is verified and the contents of the encrypted ACK prob within time out, the originator conclude that the link between itself and the suspicious node does not

contain a wormhole tunnel. The originator keeps up the neighbor relationship with this node and acknowledges data from that node. If one of the two nodes judges the remote node or the content of ACK prob as suspicious, the originator concludes that the link is still suspicious.



In this case the originator restarts communication with that node after a randomly chosen time. When this time expires, the originator proceeds again with the exchange of Probing and ACK prob packets. If the result of this exchange leads to the conclusion of at least one suspicious state, the originator regards this connection as a wormhole tunnel.

TIMEOUTS [7]

The value of the timeout has to be calculated carefully in order to avoid false

Decisions. If the timeout value is set too small, normal nodes can be mistakenly suspected Then again, if the timeout is set to a very large value, it turns out to be difficult to identify any wormhole assault. The timeout setting is related to whether it can distinguish the normal wireless transmission range of a single hop. Timeout can be then defined as follows:

Timeout = 2R/V+ Tproc

where R denotes the maximum transmission range of each node or radio coverage. V is the propagation speed of the wireless signal. In our solution, if a link is regarded as suspicious, the link is given another chance to prove its legitimacy rather than being subject to immediate coercive measures.

This chapter discuss, AODV under Wormhole attack .The chapter also contain proposed algorithm "Detection and Removal of Wormhole attack" and its explanation. It is believed that the proposed scheme will have a positive impact in malicious node detection and prevention of wireless Mobile Ad hoc Networks.

5. SIMULATION TOOL & RESULTS

MATLAB is a high-level language and interactive environment for numerical calculation, perception and programming. Utilizing MATLAB, we can investigate data, create algorithm, calculations and create models and applications. The language, tool and built –in math function enable us to explore multiple approaches and research a solution faster than with spreadsheets or traditional programming language, such as C, C++, or Java. More than million of engineers and scientists in industry use MATLAB, the language of technical computing. In this implementation work MATALAB R2009a is used the version is 7.8.0.347.

IMPLEMENTATION OF AODV PROTOCOL IN MATLAB.

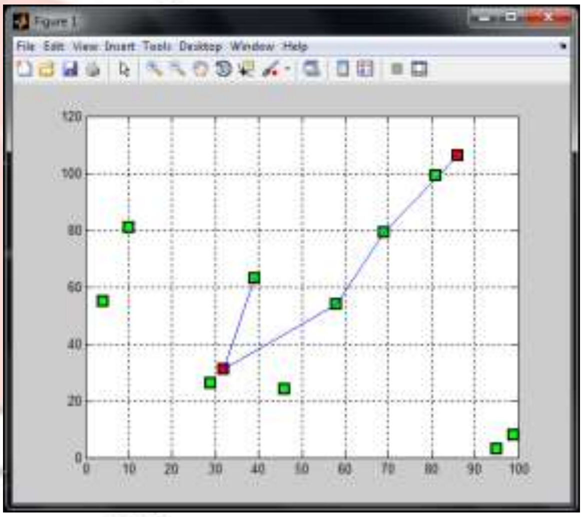
Node placement

Node placement module is used for placement of mobile nodes .Author consider the node located at apposition which is defined by X and Y co-ordinate. For randomness nature X and Y Co-ordinate is defined as random by help of random function available in MATLAB2009.

```
for  i = 1:1:Max
n(i,:) = randint ( 1,2,[2 100] )  ;
end
```

WORMHOLE ATTACK IN AODV ROUTING PROTOCOL

Wormhole attack is severe attack to AODV routing protocol. The malicious node falsely advertises that it has a one hop count from the destination. The sender node sends the data through the suspicious links and malicious node tunnel the data to another malicious node in the network.



The results of proposed algorithm "Detection and Removal of Wormhole attack " are show through the command prompt view in MATLAB. In the Fig. the result of simulation are shown .The malicious nodes are detected between the source and destination. The malicious node falsely advertises the shortest path as shown in the Fig. The malicious nodes are detected and removed successfully .The Trusted path is established between the source node and the destination node in the network.

The proposed algorithm successfully detected list of malicious node in the network in Fig .When the list of malicious nodes are updated then it is broadcast to the neighboring node and each node updates their malicious list.

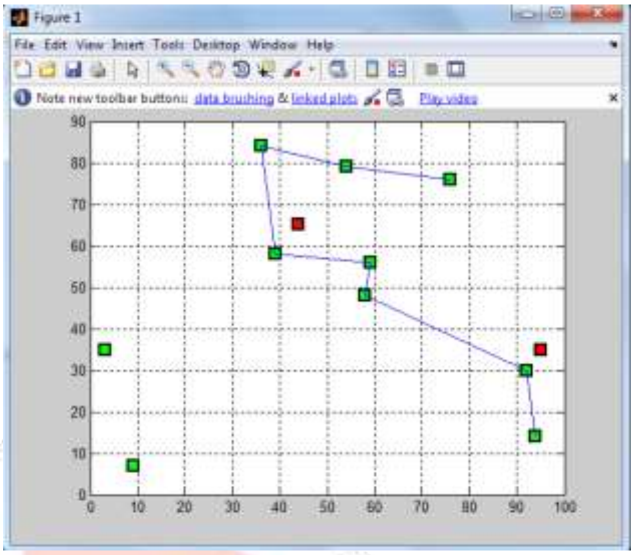
PROPOSED ALGORITHM IMPLEMENTATION

Proposed Algorithm Implementation for detection and removal of malicious nodes in Mobile Ad hoc Network. Wormhole attack is severe attack to AODV routing protocol .The Wormhole Attack is using packet encapsulation.

Command prompt view of proposed Algorithm

The malicious node falsely advertises that it has a one hop count from the destination. The sender node sends the data through the suspicious links and malicious node tunnel the data to another malicious node in the network.

The results of proposed algorithm “Detection and Removal of Wormhole attack “ are show through the command prompt view in MATLAB. The proposed algorithm successfully detected list of malicious node in the network in Fig 6.6 .When the list of malicious nodes are updated then it is broadcast to the neighboring node and each node updates their malicious list.



6. FUTURE & CONCLUSION

It includes the conclusion made during the complete research work and future work required to be done. Mobile Ad hoc Networks (MANET) are characterized by multi hop wireless connectivity, infrastructure less environment and frequent changing topologies. . In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSDV, DSR, and AODV. The work in the thesis tried to analyze, Wormhole attack in AODV routing protocol in the mobile ad hoc network. Although many solutions have been proposed but still there is a requirement of routing protocol which not only provide efficient routing but can also provide security to Mobile Ad hoc Network (MANET). The work in the thesis tried to analyze wormhole attack with some different scenarios with respect to performance parameter of end to end delay and network load. These are exposed to both internal and external attacks as there is decentralized security mechanism. In future a lot of research work is still needed in this area. The Proposed work discovers and analyzes the impact of Wormhole attack in MANET using AODV protocol. There is need to develop a secure protocol for detection for all types of attack such as black hole attack, byzantine attack , flooding attack.

REFERENCES

1. C.E. Perkins, P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers," Proceedings of ACM SIGCOMM Communications Architectures, Protocols and Applications, 1994.

2.P.Krishna,N.H.Vaidya,M.Chatterjee, D.K.Pradhan, "A cluster-based approach for routing in dynamic networks," ACM SIGCOMM Computer Communication Review, pp.49–65, 1997.

3. B. Bellur, R.G. Ogier, A reliable, "efficient topology broadcast for dynamic

networks," Proceedings of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99), pp. 178–186, March 1999.

4. Frank Stajano and Ross J. Anderson, "The resurrecting duckling: Security issues for Ad hoc wireless networks", pages 172–194. Lecture Notes in Computer Science, 1999.

5. C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, 1999, pp. 90-100.

6. A. Qayyum, L. Viennot, A. Laouiti, "Multipoint relaying: an efficient technique for flooding in mobile wireless networks," Project HIPEERCOM, INRIA, Technical Report Research Report RR-3898, February 2000.

7. Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. pp.2-17.

8. Charles Perkins, Elizabeth Royer, Samir Das, Mahesh Marina "Performance of two on-demand Routing Protocols for Ad-hoc Networks", IEEE Personal Communications, February 2001, pp. 16-28.

9. B. Dahill, B.N. Levine, E. Royer, C. Shields, "A secure routing protocol for ad

hoc networks", Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS- 2001-037, August 2001.

10. D. Johnson, D. Maltz, J. Broch, "The dynamic source routing protocol for multihop wireless ad hoc networks," Ad Hoc Networking, Addison-Wesley, 2001.

11. J.Zhen and S. Srinivas. "Preventing replay attacks for secure routing in ad hoc Networks". In ADHOC-NOW, LNCS 2865, pages 140–150, 2003.

12. Y. C. Hu, D. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad

Hoc Network Routing Protocols,” Proc. ACM Wksp. Wireless Sec., San Diego,CA,Sept. 2003.

13. Y.C. Hu, A. Perrig, D.B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” 22nd INFOCOM, pp.1976–1986, 2003.

14. S. Capkun, L. Buttyan, and J.-P. Hubaux, “SECTOR: Tracking of Node Encounters in Multihop Wireless Networks,” Proc. ACM Wksp. Sec. of Ad Hoc and Sensor Networks, Fairfax, VA, Oct. 2003.

15. H.L.Nguyen , U.T .Nguyen, “Study of Different Types of Attacks on Networking System”Mobile Communication and Learning Technologies , Apr,2006.

16. Y. Zhang et al., “Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006, pp. 247–60.57

17. Y. C. Hu, D. Johnson, and A. Perrig, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” Proc. ACM Wksp. Wireless Sec., San Diego, CA, Sept. 2003.

18. Sunil Taneja and Ashwani Kush“A Survey of Routing Protocols in Mobile Ad Hoc Networks”.