International Journal of Research in Computer Science
eISSN 2249-8265 Volume 2 Issue 1 (2011) pp. 21-27

www.ijorcs.org

PERFORMANCE EVALUATION OF AODV PROTOCOL UNDER PACKET DROP ATTACKS IN MANET

Suchita Gupta[1], Ashish Chourey[2]
*Assistant Professor, Department of Information Technology
Gyan Ganga Institute of Technology & Management, Bhopal, Madhya Pradesh, India

Abstract: *Mobile Ad hoc Network (MANET) is self configuring network of mobile nodes connected by wireless links and is considered as network without infrastructure. In MANET, routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that all nodes are fully cooperative. As the structure of MANET is open and the limitation of mobile nodes to operates on the battery-based energy, some nodes may not cooperate correctly. Such non-cooperation of nodes in routing is referred as routing misbehavior. After becoming part of source route, these nodes start refusing to forward or drop data packets thereby degrades the performance of network. In this paper, an approach named "Performance evaluation of packet drop attack in MANET" is proposed that can be integrated on top of any source routing protocol. This approach deals with routing misbehavior and consists of detection and isolation of misbehaving nodes and reduces the network traffic. The concept behind the packet drop is to reduce the traffic and identify the malicious node in the network.*

Keyword: *Adhoc network, Association based AODV, packet drop, malicious nodes.*

I. INTRODUCTION

A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links [1]. There are no base stations, access points, and any centralized control equipment. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. Nodes can communicates directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, noncooperation may occurs which can severely degrades the performance of network. MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Those attacks are more dangerous that are initiated from inside the network and because of this the first defense line of network become ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect. Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes.

II. BACK GROUND

A. AODV Protocol

Adhoc On demand Distance Vector is a protocol for routing in mobile ad-hoc networks [2]. In a nutshell, it works as follows: AODV shares DSR's on demand characteristics in that it also discovers routes on an "as needed" basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a RREP back to the source and, subsequently, to route data packets to the destination. AODV uses destination sequence numbers as in DSDV to prevent routing loops and to determine freshness of routing information. These sequence numbers are carried by all routing packets. The absence of source routing and promiscuous listening allows AODV together only a very limited amount of routing information with each route discovery. Besides, AODV is conservative in dealing with stale routes. It uses the sequence numbers to infer the freshness of routing information are discarded even though they may still be valid.

AODV also uses a timer-based route expiry mechanism to promptly purge stale routes. Again if a low value is chosen for the timeout, valid routes may be needlessly discarded. In AODV, each node maintains at most one route per destination and as a result, the destination replies only once to the first arriving request during a route discovery.

B. Common Security Threats

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks [3] [6] according to the attack means A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. The goal of active attack may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. This makes active attacks a less inviting option for most attackers. Yet, it may still be a real alternative when large amounts of money are at stake such as in commercial or military environments. The following is a list of some types of active attacks that can usually be easily performed against an ad hoc network.

***Black hole*:** a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [4].

Wormhole: In the wormhole attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them there into the network [5]. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

Rushing attack: This kind of attack is a malicious attack that is targeted against on demand routing protocols that use duplicate suppression at each node, like AODV [3]. An attacker disseminates ROUTE REQUESTs quickly throughout the network, suppressing any later legitimate ROUTE REQUESTs when nodes drop them due to the duplicate suppression. Thus the protocol cannot set up a route to the desirable destination.

Sinkhole*:* where an attacker tries to attract all the data sent by its neighbors'. This attack is the basis for example, eavesdropping [7]. Sinkhole attackers present themselves to adjacent nodes as the most attractive relay in a multi-hop route.

Spoofing: By masquerading as another node, a malicious node can launch many attacks in a network [8]. This is commonly known as spoofing. Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets. Spooling combined with packet modification is really a dangerous attack.

***Routing table overflow*:** In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes [9]. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation.

III. PROBLEM STATEMENT

The objective of this paper is to identify and isolate the malicious nodes, to improve the performance of the AODV protocol under packet drop attack scenario in terms of throughput, packet data ratio and dropped data packet. A selective packet drop [10] is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination. As an example consider the scenario in figure 1. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 act as the intermediate nodes. Node 5 acts as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighboring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others. This type of attack is very hard to detect as the malicious nodes pretend to act like a good node. The selective packet dropping attacks have a great negative influence over the performance metrics of conventional protocols. In this article we evaluate the performance of the AODV protocol under packet drop attack scenario. To improve the performance we dynamically detect the malicious node and choose different route to improve throughput, packet delivery ratio.

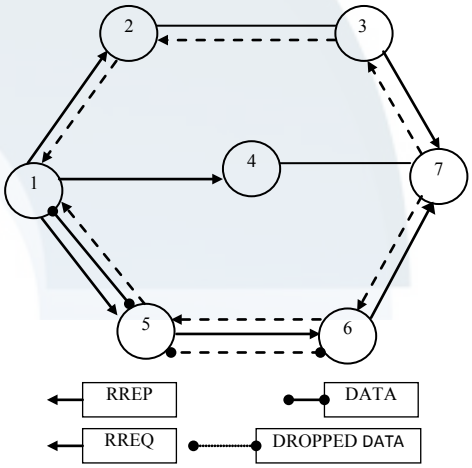

Figure 1: Selective Packet drop attack scenario

IV.LITERATURE REVIEW

Over the past few years, a variety of routing protocols targeted specifically at the ad hoc networking environment have been proposed, but little information about the effects of security exposures in terms of network performance has previously been available. This paper provides a simulation study that illustrates and analyzes the performance of AODV protocol under selective packet drop attack.

Marti, Guiti, Lai and Baker [11] proposed the watchdog and Pathrater scheme in which watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations, it is highly effective in source routing protocols, such as DSR. The path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the Network. Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior.

Buchegger and Le Boudec [12] present the CONFIDANT protocol. The CONFIDANT protocol works as an extension to reactive source routing protocols like DSR. The basic idea of the protocol is that nodes that does not forward packets as they are supposed to, will be identified and expelled by the other nodes. The protocol consists of four components. Each node Monitor the behavior of its next hop neighbors in a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node's rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial packet dropping.

The Grudger Protocol As explained in [13] it is an application from a biological example proposed by Dawkins proposed a biological example, which explains the Survival chances of birds grooming parasites off each other's head. Dawkins introduces three categories of the birds namely:

- Suckers which are good natured, helpful and favor others by grooming parasites off others head.
- Cheats which get help from others but fail to return the favor.
- Grudger who starts out being helpful to every bird, but bears a grudge against those birds that don't return the favor and subsequently no longer help them.

In an ad hoc network, grudger nodes are introduced which employ a neighborhood watch by keeping track of what is happening to other nodes in the neighborhood, before they have a bad experience themselves. They also share information of experienced malicious behavior with friends and learn from them.

Michiardi and Molva propose the CORE scheme [14] [15]. In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbors past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended.

V. IMPLEMENTATION WORK

This section presents the Association based routing which is to be applied over the AODV protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network.

For each node in the network, a trust value is calculated which represent its reliability level. Based on the trust value calculated and threshold parameters they are classified in to three types as discussed below.

A. Nature of Association between neighboring nodes in an Ad Hoc Network

In our proposed scheme we classify the Association among the nodes and their neighboring nodes in to three types as below. In an adhoc network the Association between any node **x** and node **y** will be determined as follows.

UNKNOWN

- Node x have never sent/received any messages to/from node y
- Trust levels between them are very low.

- Probability of malicious behavior is very high.
- Newly arrived nodes are grouped in to this category.

KNOWN

- Node x have sent/received some messages to/from node y
- Trust levels between them are neither low nor too high.
- Probability of malicious behavior is to be observed.

COMPANION

- Node x have sent/received plenty of messages to/from node y
- Trust levels between them are very high.
- Probability of malicious behavior is very less.

The above Associations are represented in an Association table which is part of every node in the adhoc network. For an example the Association table of node 1 in the figure 2, is given in Table 1.

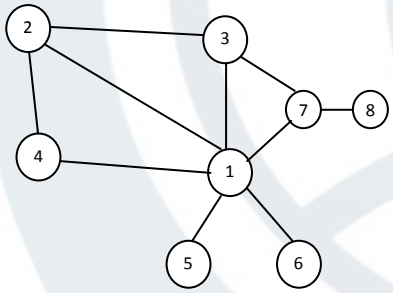

Figure 2: Nodes in Adhoc Network

Table 1: Association Table for node 1 in Figure 2

Neighbors	Nature of Association
2	C
3	C
4	K
5	C
6	K
7	UK

B. Association estimator technique

The Association status which we discussed in the previous section depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. We propose a very simple (1) for the calculation of trust value between any two node in the network.

$$\mathbf{TV} = \tan(\mathbf{R1} + \mathbf{R2} + \mathbf{A}) \ldots. (1)$$

Where

TV = Trust value

$$R1 = \frac{\text{No.of packets forwarded successfully by neighbor node}}{\text{Total no of packets to be forwarded by neighbor node}}$$

If the denominator is not zero and R1 is less than the chosen threshold (R1<1) & not zero then it can cause selective packet drop attack.

$$R2 = \frac{\text{No.of packets received from neighbor node But originated from other nodes}}{\text{Total no of packets received from that node}}$$

A = Acknowledgement. (0 or 1) if the acknowledgment is received for data transmission from the destination then nodes in that path are assigned value 1 else value 0 is assigned.

The threshold trust level for an unknown node to become a known to its neighbor is represented by TK and the threshold trust level for a known node to become a companion of its neighbor is denoted by TC.

The Associations are represented as

A (node x → node y) = Companion, if T ≥ TC

A (node x → node y) = Known, if TK ≤ T < TC A (node x → node y) = Unknown, if 0 < T > TK Where T = Threshold

K = known, UK= unknown,

C = companion

Also, the Association between nodes is asymmetric, (i.e.) R (node x → node y) is an Association evaluated by node x based on trust levels calculated for its neighbor node y. R (node y → node x) is the Association from the friendship table of node y. This is evaluated based on the trust levels assigned for its neighbor. Asymmetric Associations suggest that the direction of data Flow may be more in one direction. In other words, node x may not have trust on node y the same way as node y has trust on node x or vice versa. The Threshold parameters are design parameters. Simulation is to be carried out with suitable values or all the parameters and the threshold trust levels so as to obtain optimum performance. There is a tradeoff between offering good security in adhoc networks and overall throughput of the network. Hence, choosing an optimal value is crucial for the good functioning of the network.

C. Routing Mechanism

When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST (RREQ) to all the neighboring nodes. The ROUTE REPLY (RREP) obtained from its neighbor is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a Companion, then that path is chosen for message transfer. If its one-hop neighbor node is a known, and if the one hop neighbor of the second best path is a companion choose C. Similarly an optimal path is chosen based on the degree of Association existing between the neighbor nodes.

Table 2: Path Chosen Based On Proposed Scheme

Next hop neighbor in the best path P1	Next hop neighbor in the next	Action Taken
C	**C**	C is chosen in P1 or P2 based on the length of path
C	K	C is chosen in P1
K	C	C in path P2
K	K	K is chosen in P1 or P2 based on
		the length of the path
C	U K	C is chosen in P1
U K	C	C in path P2
U K	U K	UK is chosen in P1 or P2 based on the
K	U K	K or UK is chosen on the length
U K	K	UK or K is chosen based on

C=Companion, K=Known, UK=Unknown

The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the AODV protocol if all the nodes in the ad hoc network are companions.

VI.SIMULATION SET UP

The simulation is implemented on Network Simulator 3, a simulator for mobile adhoc networks [17]. In MANETs, the entity mobility models typically represent nodes whose movements are completely independent of each other in un- cooperative fashion, e.g. the Random Way Point (RWP) model. The results of these runs were averaged to produce the graphs shown below. Table 3 provides a summary of the chosen simulation parameter values.

Table 3: Simulation Parameters

Parameter	**Value**
Examined Protocol	AODV
Traffic type	Constant bit rate(UDP)
Transmission range	100 m
Packet size	512 bytes
Data rate	100 kb/s
Pause time	10 s
Maximum speed	20 m/s
Minimum speed	1m/s
Simulation time	900s
Antenna type	Omni Antenna
Area	1000 m * 1000 m
Number of nodes	50
Movement Model	Random waypoint
Maximum Malicious node	20
Types of attack	Selective packet drop

VII. RESULT AND ANALYSIS

For the performance analysis of the Association based AODV protocol the throughput is compared with the standard AODV in presence of the malicious nodes.

A. Effect of Packet drop Attack on the Packet Delivery Ratio

PDR is the packet delivery ratio in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources (CBR, "application layer") and the number of received packets by the CBR sink at destination.

Figure 3 show the effect of the packet drop attack on the packet delivery ratio measured for the AODV protocol when vary the malicious nodes. The result shows both the cases, Standard AODV and AODV .It is measured that there is the reduction in the packet delivery ratio when there are the malicious nodes in the network.

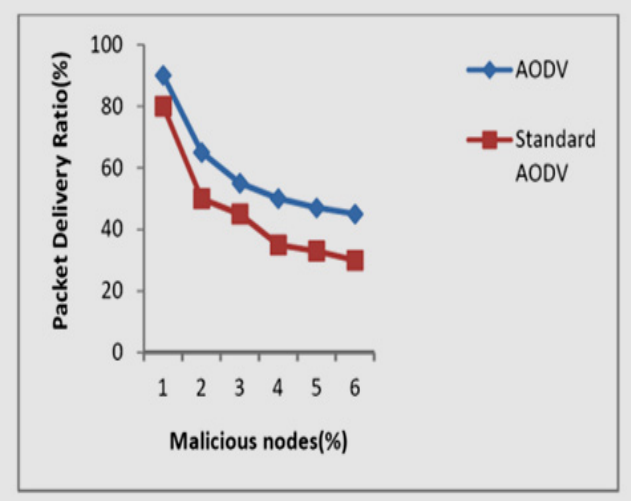

Figure 3: Comparison of Packet Delivery ratio vs. malicious nodes

B. Effect of Dropped Packet

We conducted another simulation to determine the percentage of dropped data packets for proposed and standard protocol. When no malicious nodes are present the standard AODV has less dropped data packets but these changes when the number of malicious nodes increases. The results are shown in Figure 4.

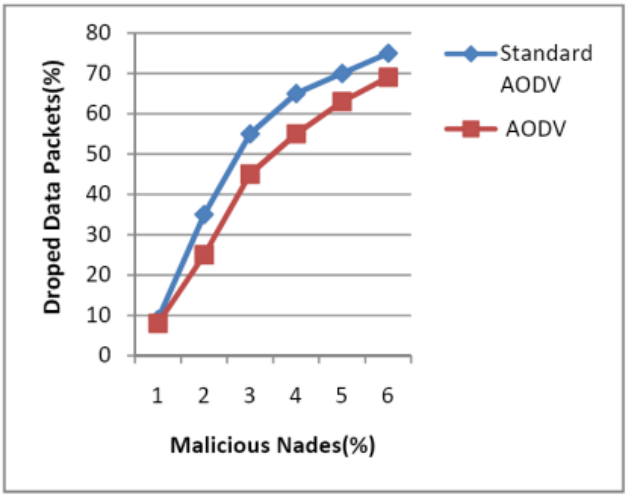

Figure 4: Comparisons of Dropped Data Packets vs. malicious nodes

C. Effect of Packet drop Attack on Overhead

The routing overhead is increased significantly when the network topology changes faster or there are a high percentage of malicious nodes in the network. In both scenarios, a large number of probe messages have to be sent out to finalize the node states. The overhead can be reduced dramatically if probing messages normal piggyback data packets. The result is shown in figure 5.

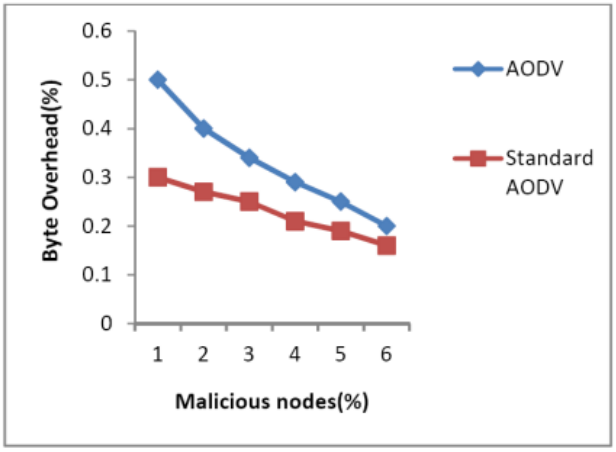

Figure 5: Comparisons of Bytes Overhead vs. malicious Nodes

D. Effect of Packet Drop Attack on the Network

Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets. The result is shown in figure 6.

E. Effect of Packet Drop Attack on the Average Latency

Average Latency gives the mean time (in seconds) taken by the packets to reach their respective destinations.

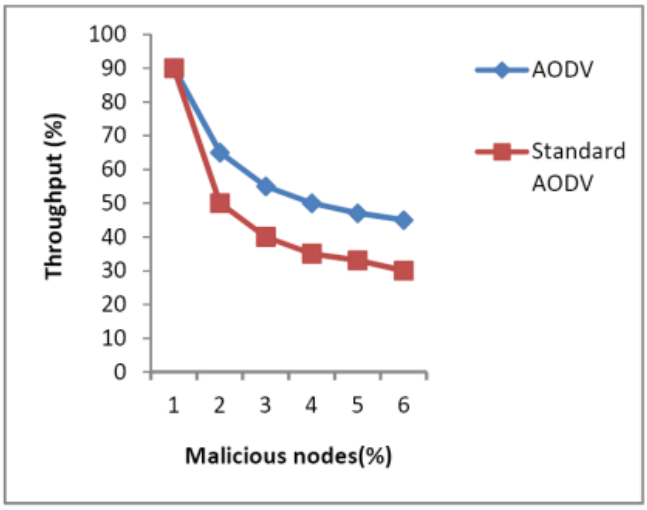

Figure 6: Comparison of throughput vs. malicious nodes

The simulation results in Figure 7 illustrates that the average latency are slightly higher than the conventional one due to the trust based routing.

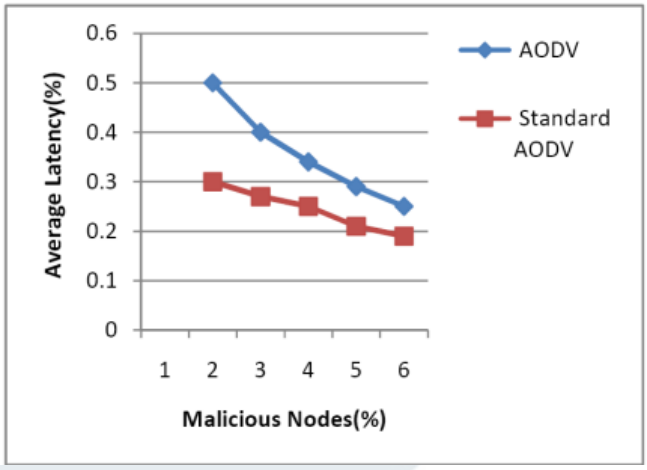

Figure 7: Comparision Of Average Latency

VIII. CONCLUSION

With development in computing environments, the services based on Ad Hoc Networks have been increased. Wireless Ad Hoc Networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In this paper, we focus on an attack packet drop. The malicious nodes that are the part of network, they receive the packet and drop them without forwarding it to the other nodes. This paper provides the simulation study and illustrated the effect of these active attacks on the network performance. If the security in the AODV routing protocol is nonexistent, the network can have no security against packet drop attack and can disable the entire network. The packet drop attacks depends number of malicious nodes in the network. As the malicious nodes increase the performance of the networks gradually drops.

IX. REFERENCES

[1] C. Siva Ram Murthy and B. S. Manoj "Ad Hoc Wireless Networks: Architectures and Protocols" Prentice Hall, 2004.

[2] Perkins CE, Royer EM. "Ad-hoc on-demand distance vector routing" Proceedings of 2nd IEEE Workshop on Mobile Computer Systems and Applications, February 1999.

[3] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", 2006 Springer.

[4] Dokurer, S. Ert, Y.M., Acar, C.E SoutheastCon, "Performance analysis of adhoc networks under black hole attacks". Proceedings IEEE Volume, Issue, 22- 25 March 2007 Page(s):148 — 153.

[5] Hu YC, Perrig A, Johnson DB. "Packet leashes: A defence against wormhole attacks in wireless ad hoc networks" Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[6] Hoang Lan Nguyen, Uyen Trang Nguyen" A study of different types of attacks on multicast in mobile ad hoc networks" Ad Hoc Networks 6 (2008) 32–46, Elsevier B.

[7] Burg A. "Ad hoc network specific attacks" Seminar Adhoc networking: Concepts, Applications, and Security. Technische Universitat Munchen, '03..

[8] Karlof C, Wagner D. "Secure routing in wireless sensor networks: Attacks and countermeasures" Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications May 2003

[9] Jøsang A. "The right type of trust for distributed systems" Proceedings of ACM New Security Paradigms Workshop, September 1996.

[10] N.Bhalaji and Dr.A.Shanmugam "Reliable Routing against Selective Packet Drop Attack in DSR based MANET " in JOURNAL OF SOFTWARE, VOL. 4, NO. 6,AUGUST 2009.

[11] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker."Mitigating routing misbehaviour in Mobile ad hoc networks" Proceedings of MOBICOM 2000. Pages 255-265.

[12] Sonja Buchegger and Jean-Yves Le Boudec: "Performance analysis of the CONFIDANT protocol" Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing'02. p.p:226 – 236.

[13] Sonja Buchegger and Jean-Yves Le Boudec. "Nodes Bearing Grudges: Towards Routing Security, Fairness androbustness in Mobile ad hoc networks". Proceedings of theTenth Euromicro Workshop on Parallel, Distributed and Network–based processing. Canary Islands, Spain. January2002. IEEE Computer Society. Pages 403 – 410.

[14] P. Michiardi and R. Molva. Preventing denial of service And selfishness in adhoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[15] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile Adhoc networks. In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, pages 107–121, Portorosz, Slovenia, September 2002.

[16] Prashant Mohapatra, Srikanth V. Krishnamurthy, a book on "AD HOC NETWORKS Technologies and Protocols"2005

[17] Kevin Fall, Kannan Varadhan: The ns manual, http://www.isi.edu/nsnam/ns/doc/index.html