International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.5., 2015 (Sept.-Oct.)

RESEARCH ARTICLE

ISSN: 2321-7758

SECURE ROUTING AGAINST MALICIOUS ATTACKER IN SPONTANEOUS MANET

SHIVANI RAJPUT[1], Prof. RATAN SINGH THAKUR[2]

[1]M.Tech. Pursuing, Dept. of CSE, Rajiv Gandhi proudyogiki Mahavidyalaya, Bhopal, Madhya Pradesh, India

[2]Head of Department, CSE Rajiv Gandhi proudyogiki Mahavidyalaya, Bhopal, Madhya Pradesh, India

SHIVANI RAJPUT

ABSTRACT

The Malicious attacker nodes in Mobile Ad hoc Network (MANET) are disputes the normal routing performance that degrades the network performance. The malicious nodes are always mystify intermediate nodes in routing procedure because these nodes are only receive and forward reply of surrounding neighbor. In this research we proposed a new security algorithm against malicious attack in MANET. The proposed security method of finding attacker is based on the link detection method for data forwarding. This method not only identified the malicious nodes but also prevent from routing misbehavior from malicious nodes. The attacker is identified from heavy data dropping and their prevention is possible by selecting the next possible route where attacker does not exist in connected link between sender and receiver. The intermediate nodes are identified the attacker through confirm optimistic reply of malicious node/s in dynamic network. The proposed security IDS (Intrusion Detection and prevention) is securing the MANET and may be possible improves the network performance as equal to normal network performance. The network performance is measures through performance metrics like throughput, routing packets flooding and proposed mechanism secures routing that provides zero packet dropping in presence of malicious attacker.

Key words:- Malicious Attacker, routing, Security, MANET, network performance.

INTRODUCTION

Mobile Ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network [1]. Mobile ad hoc network is a group of wireless mobile computers (or nodes); in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. The attackers in MANET are easily affected the normal network performance because of absence of coordination system [2]. There are two types of attacks in network first is *active* and another one is *passive.* Active attackers are very harmful because they are hammering and distort the whole network performance but their detection and prevention is possible but passive attackers are not distort complete network performance but slightly amount of data is affected by that this kind of attacker are not recognized easily. The attacker's classification in detail mentioned in [2].

In active attack, *malicious nodes* or attacker nodes in network are responsible for packets dropping due to routing misbehavior [1]. The routing performance of network is degrades because of heavy packet dropping. Mobile and self organizing characteristics of MANET makes an excellent prospect, however, it faces a lot of security issues. For example, key management and authentication, routing security, intrusion detection, and enhance cooperation. Intrusion detection is security technology, which finds that a network or system whether there is any breach of security strategy and the sign of invasion that is through network or computer system from a number of key points in the collection of information and analysis. The many IDS schemes [3] identified the attacker misbehavior and obstruct their existence. The IDS Security scheme not only detected but also prevent from attacker.

These routing protocols [4, 5] in MANET are similar to and come as a natural extension of those for the wired networks. In proactive routing, each node has one or more tables that contain the latest information of the routes to any node in the network. The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately.

The proposed secure IDS is provides the attacker free routing by identified it through calculate the path length selected by the attacker false reply. The security system is apply the security procedure to that wrong path and identified the destination reachability from that path. The destination confirmation is also confirm the data is not received then, identified the malicious nodes and blocks their functioning for providing secure communication.

Related Work

It has been observed that although active research is being carried out area of security in MANET, the proposed solutions are not complete in terms of effective and efficient routing security against malicious attack but slightly strike the idea of new research. The some previous works are discussed in this section.

Wherever In this paper [1] can establish a secure established environment for data delivery and services sharing among users. A every new node is able to join the network because it knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification. Spontaneous ad hoc networks require well defined, efficient and user-friendly security mechanisms. Tasks to be performed include: user identification, their authorization, address assignment, name service, operation, and safety.

In this paper [6], proposed new secure system called Audit based Misbehavior Detection, (AMD) which achieves per-packet behavior evaluation without incurring a per-packet per-hop cost. AMD is a comprehensive solution that integrates identification of misbehaving nodes, reputation management, and trustworthy route discovery in a distributed and resource-efficient manner. We show that AMD can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, a behavioral audit process efficiently locates these nodes.

This paper [7] proposes a general security framework for monitoring and reacting to disruptive attacks. It includes a collection of functions to detect anomalies, diagnose them, and perform mitigation. The measures are deployed in each node in a fully distributed fashion, but their collective impact is a significant resilience to attacks, so that the actors can disseminate information under adverse conditions node whose aim is to disseminate a message to as many new nodes as possible faces a number of challenges.

First, if it tries to deduce the state of communication availability (and the potential threats) by observing its vicinity it will have a local and very restricted view of the world. Second, it is difficult to have a model of an attacker in both space and time.

Third, the dissemination protocols, including one that we use for illustration of ideas in this paper, have a tendency that they can spread the impact of an attack in space and in time.

In this paper [8], we propose a risk aware response mechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation method. In order to measure the risk of both attacks and countermeasures, we extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, we also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk aware approach.

In this paper [9], we focus on the latter aspect, hereinafter referred to as neighbor position verification (NPV for short). Specifically, we deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services.

In [10], an authenticated distance bounding technique called MAD is used. The approach is similar to packet leashes at a high level, but does not require location information or clock synchronization. But it still suffers from other limitations of the packet leashes technique.

In the Echo protocol [11], ultrasound is used to bound the distance for a secure location verification. Use of ultrasound instead of RF signals as before helps in relaxing the timing requirements; but needs an additional hardware.

Proposed Secure IDS Routing

The proposed research is very useful in field of computer science to evaluate the network performance in case of attack and Secure Intrusion Detection and Prevention (IDS) security algorithm. At present network, security is one of the challenging task in without central administration based network now on in MANET i.e. no admin in network security is major concern. In **figure 1** the actual path in between sender to receiver is S-A-D of minimum hop count but the malicious attacker M is forward the false reply to sender is "destination exist" and the data is deliver through that attacker node but the attacker is wait for the data and if it receives it drop the data. Attacker does this kind of routing misbehavior to every sender in network by that the whole network performance is dump in presence of attacker.

In this research, an exhaustive simulation for MANET will done by using AODV routing protocols and the effect of the presence of routing misbehavior will also simulated. Significant performance parameters such as infection rate throughput, delay, node density and packet delivery ratio. This research is focuses on how performance of network will affect under routing misbehavior attack in a network and how the proposed SDP is block the malicious activities of attacker and provides secure routing after proving the valid variables value.

X_n=Y_n.........................eq.(1), x ≤y

n=1 means one sender and one receiver sender and so on.

it implies that the difference in of these two path variable is equal to zero.

$X_n - Y_n = 0$ ....eq. (2)

The path between the nodes is not identified correctly but in this research verifies the path i.e. selected by attacker for dropping the data packets.

Proposed Secure IDS Functioning

Number of nodes (N_m) = 50 // number of nodes in path length $X_n = N_m+1$

Routing Protocol = AODV

Type of attacker = Malicious attacker (Packets Dropping)// M_A

Security Provider = IDS (Intrusion Detection System) // Security Procedure

Nodes Radio Range (RR) = 250m // in meters unit

Step1: Sender has sending the request (RREQ) to all intermediate nodes that are directly in radio range of senders (S_s).

s=1,2,3...... // depend on number of senders

Step2: Add the path entry in routing table if Destination (D_d) is found, otherwise forward the request to next neighbors and sustaining the path length information up to destination.

d=1,2,3....... // depend on number of destinations

Note:- Source and Destination communication is unicasting that's why in both number of sources ahs only one destination.

Step 3: If Destination (D_d) is found then select the route of minimum path length and deliver data through that minimum path length (X_n) and also one variable Y_n stores X_n value for confirming data delivery up to destination.

1. Data packets containing the value of path length and each length count the degrades X_n from Y_n.
2. $\sum X_n = (X_1, X_2, X_3 \ldots X_n)$ up to destination is Minimum then select for data sending with holding the value of (Y_n) and also next route of hop count $X_1, X_2, X_3 \ldots X_n \geq$ Min path length then identified the possibility of attacker.
3. The $X_1, X_2, X_3 \ldots X_n \geq$ Min path length is decided by secure IDS in presence of attacker.

Step4: Compare the routing performance through secure IDS system to calculate path length through X_n and Y_n , if these variable difference is **zero** matched (eq. 2). It means no attack in the network; path is secure, and data packets forwarding is proper in between S_s to D_d.

Step8: The secure IDS (Intrusion Detection system) verify if routing information of path length selected by attacker is not matched related to actual routing information of path length, that confirm some routing misbehavior activity occurs in the network through malicious nodes.

Step5: If the path length calculation is provides some negative values, and X_n , Y_n (eq. 2) conditions are not matched. That confirms the attacker presence M_A (M malicious modes)

If path length $X_1, X_2, X_3 \ldots X_n \neq Y_n$.

It means no data is delivering through that path up to destination, insert the table new entry in routing table which has contain path information to destination. Otherwise go to step 2

Step6: If next path length is countable and X_n value is not reduced from Y_n is factual condition, forward data through that link or path and data forwarding information is false then send the data packet for checking the reliability through proposed IDS security scheme.

Step9: The secure IDS prevention scheme block that node i.e. attached to that path and change the path, forward data packet. Also forward the nodes identification in network by that the attacker neither or nor selecting in routing procedure.

Step 10: If the attacker is be present in selecting path for data delivery then avoids that path and preferred another suitable paths established by AODV.

Attacker exist path length $X_1, X_2, X_3 \ldots X_n$ = Min then,// selects attacker free path

Select route of path length $X_1, X_2, X_3 \ldots X_n \geq$ Min // avoids shortest path

Step11: Then forward data packet until send all data packet reach to destination otherwise no attacker is exist in network.

Step7: But data packets forwarding and route information is correct then it is valid condition of routing in network and go to step 2.

Step 12 Exit

The example of proposed security system working is mentioned below in presence of attacker. The proposed scheme is work to count whole length of path from source to destination. If the more then more than one path is established then select shortest path in between S_s to D_d. In this figure 1 the receiver is reply to sender about shortest path but malicious node M is forward the false route information of receiver to sender. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true or factual path.

The two variables X_n and Y_n are count use to count the length of *n* paths. In this given figure the AODV routing protocol is send the RREQ packets to all neighbors like C, M and K and these are forward the confirmation of RREQ packets by RREP packets.

If the destination is found then after selecting shortest path data sending is started and if no node is destination in that case all the nodes are forward the RREQ to next neighbor and they send RREP a packets to these nodes and this procedure is continue till the destination is not found. After the confirmation of destination data delivery is started.

Simulator Overview and Performance Measurement

Network Simulators are relatively fast and inexpensive as they allow the engineers to test scenarios that might be particularly difficult or expensive to emulate using real hardware. The example of is simulating the effects of a packets consumption or attack on a network service. These allow designers to test new networking protocols or change the existing ones in a controlled environment.

The simulation will do on the Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [12]. NS began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT (Virtual Inter Network Testbed) project at LBL, Xerox PARC, UCB, and USC/ISI. It is a discrete event simulator targeted at networking research. Network Simulation is a technique where a program models the network behavior either by calculating the interaction between the different network entities by actually capturing and playing back observations from a production network. Simulation Parameters

Simulation Parameters

The simulation parameters are mentioned in table1. These parameters are also change based on requirement so, in this table the following parameters are considered in this research.

Performance Metrics

There are following different performance metrics [4] has been considered to make the comparative study of these routing protocols through simulation.

1) **Packet Loss Percentage:** Rate of infection in network due to attacker or malicious nodes w.r.t time.
2) **Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent to propagate the data packets.
3) **Average Delay:** It indicates how long it took a packet to travel from the source to the application layer of the destination. It is measuring in mille seconds.
4) **Throughput:** This metric represents the total number of bits forwarded to higher layers per second.
5) **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

Results Analysis of Normal, Malicious and Proposed Secure IDS Routing

The results analysis of normal routing, malicious attack and proposed secure IDS is illustrated the effect of Malicious bodes in routing. The MANET routing performance is measure through performance metrics and UDP end to end protocols.

Routing Packets Flooding Analysis

The connection establishment packets is broadcast by sender through any network like wired and wireless to identified the actual destination. The flooding of connection establishment packets is needed because of destination is not directly in range of destination. In MANET nodes are continuously change their exist spot. In this graph the performance of routing packets overhead is evaluated in case of Normal Routing (Routing_Pkt_Normal), Malicious Attacker Routing (Routing_Pkt_Malicious) and proposed secure IDS Routing (Routing_Pkt_Secure). The malicious routing quantity is less because the data packets dropping is more but w.r.t data packets receiving the overhead is more. The routing packets overhead of normal routing is more as compare to proposed secure IDS because in presence of security system the sender is nor selects the path where attacker is exist. The proposed scheme improves routing performance in presence of attacker.

Throughput Performance Analysis

The nodes in MANET freely move in a surrounding area and also theses nodes are forward and received packets to neighbors. The throughput is measures the packets receiving at destination in unit time (time in Seconds consider in this research). The normal routing throughput is ceiling at time 570 packets/seconds (pkt/sec) at time 65 seconds but after that it reaches to 40 pks/sec, that implies that the packets receiving at unit time is also utmost. At malicious presence the routing throughput performance is almost negligible that shows the degradation in network performance but secure IDS routing throughput performance is improves the throughput and it reaches to 530pks/sec at the end of simulation. The proposed secure throughput is improves gradually that is the positive sigh of attacker disability and progressive network performance.

Packet Delivery Ratio (PDR) Performance Analysis

The larger quantity of data packets sending and data packets receiving from sending is decided the performance of any network. In dynamic network the topology is changing at every time instant and that makes the chances of link breakage and affect the packets receiving. The PDR performance of proposed security scheme is about 96% that illustrate that the better packets receiving as compare to normal routing PDR performance. The normal routing PDR is about 92%. The difference in normal PDR performance is only due to little less packets receiving. The attacker PDR performance is negligible because of negligible packets receiving at destination. The reason of packet dropping is malicious nodes and that attacker routing misbehavior is block by proposed secure IDS and improves routing performance of MANET.

Packets Loss Analysis from Malicious Attacker

The centralized administrator is the controller of network. In this presence the attacker in network is easily identified because it maintains the each and every information of data sending and receiving in network and also watches the network original activities. In MANET due to absence of centralized administrator, malicious nodes are easily forward the fake request of destination and drop all data packets in network. In this graph the packet loss percentage is measures only because of attacker and loss percentage at start of simulation is about 29% but after some drop percentage is reaches to 15% at the end of simulation. In case of normal routing the attacker existence is not detected but in proposed secure IDS the packet loss is **zero** that shows network fully secure from malicious attacker and provides secure routing.

Packets Drop in Presence of Malicious Attacker

The malicious attacker aim is to drop the data packets after fake reply of destination in MANET. The table 2 is mentioned that the number of malicious nodes in network that drop the data packets. These nodes are capture the data from sender but nor forwarded to receiver. The Malicious routing misbehavior is degrades packets receiving that degrades network performance. The proposed secure IDS is block the attacker routing misbehavior and no malicious node is detected in secure routing that shows the up-gradation in routing performance.

UDP End Connection Packets Received Analysis

The data packets after completing routing procedure are forwarded to transport layer. The transport layer in network has two main end to end connection protocols UDP is one of them. UDP (User Datagram Protocol) is the end to end communication protocol. The UDP communication is connection less, that meaning is without any conformation to receiver data sends by sender in network. Due to that the packets dropping chances are more that degrades UDP end packets receiving. In this graph the packets receiving analysis of three scenarios is evaluated and scrutinized that the proposed secure IDS routing is receives highest 800 packets but Malicious routing performance is very poor due to negligible packets receiving at UDP end.

Table -1 Considered Simulation Parameters

Simulator Used	NS-2.31
Number of nodes	50
Dimension of simulation area	1000m×1000m
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	CBR (5pkts/s)
Packet size	1024 bytes
Number of traffic connections	6
Node movement at max Speed	random (30 m/s)
Transmission range	250m

Vol.3., Issue.5., 2015
(Sept.-Oct.)

Table 2 Packet Drop by Malicious Nodes

Malicious Nodes	Drop Packets
15	10
36	595
37	151
38	127

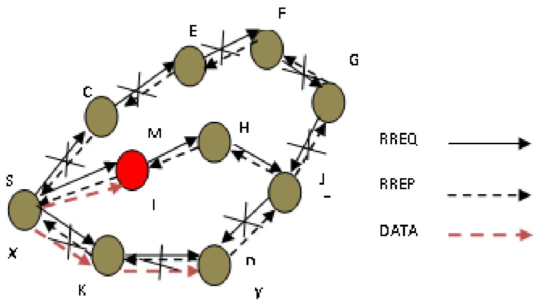

Fig. 1 Malicious node Activities

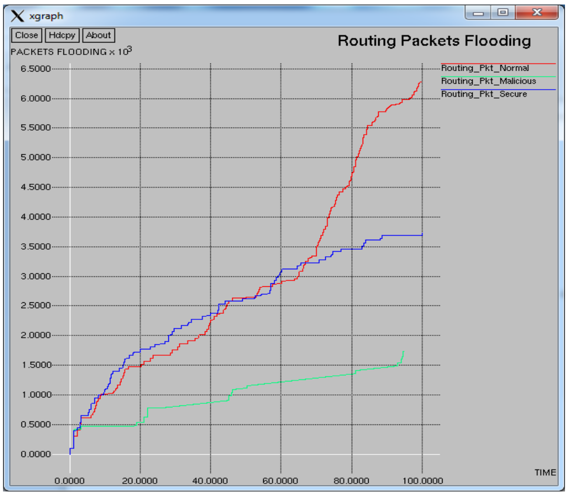

Fig. 2 Routing Packets Analysis

Fig.3 Throughput Analysis

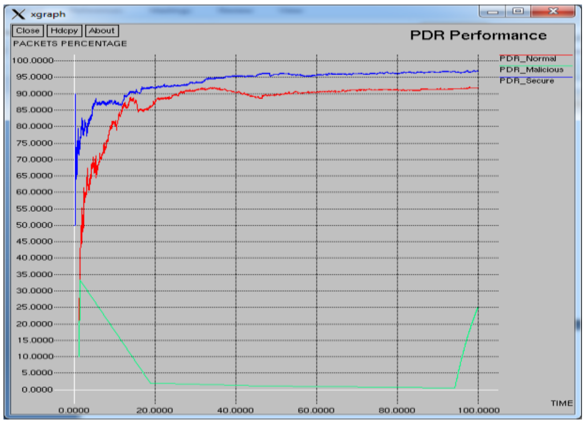

Fig. 4 PDR Analysis

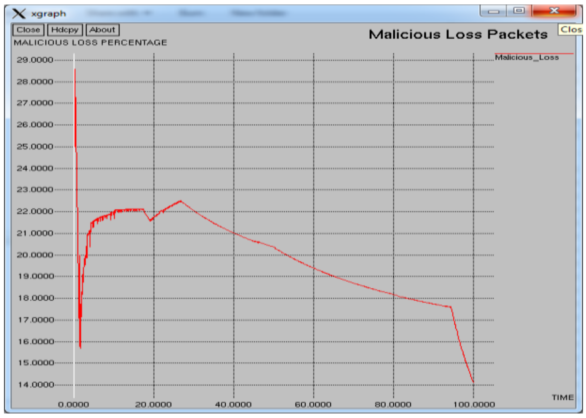

Fig. 5 Attacker Loss Analysis

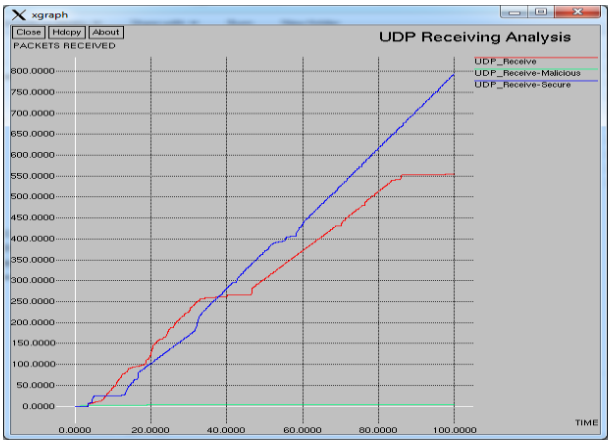

Fig. 6 UDP Packets Receiving Analysis

Conclusion and Future Extension

In ad hoc network nodes generally have a limited transmission range and so each node seeks the assistance of its neighboring nodes in forwarding packets. The nodes in network are mobile and forming a dynamic connection in between sender and receiver. The routing protocol is transferring the data in between sender and receiver through intermediate nodes. In order, to establish routes between nodes, which are farther than a single hop, specially configured routing protocol is engaged. The link establishments having a combination of normal nodes and malicious node and attacker aim is to drop data packets sending by sender to destination after connection establishment. Attacker is always tried to be a part of link for loss data packets. In this research the proposed security algorithm is identified the attacker routing malicious activities of packet dropping that degrades the routing performance of network. After detecting the malicious nodes the proposed secure mechanism is also prevent from attacker by deny the possibility of routing through malicious nodes. The proposed algorithm is improves more than 95% as compare to normal. As compare to previous works in field of routing misbehavior attack lot of research was done and it will also very effective to identify the behavior of attacker but no research will done the analysis of attack effect in TCP and UDP protocol and also not providing the complete information about the network scenario like routing misbehavior effect and malicious nodes that is the main reason of data packets drop in network.

In future apply Global Positioning System (GPS) to trace attacker easily and also aware about the all nodes of network about malicious attacker. The proposed is also applied to flooding attack and measure routing performance.

References.

[1]. Raquel Lacuesta, Jaime Lloret, Miguel Garcia and Lourdes Penalver "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, 629-641, April 2013.

[2]. Ddll A.K. Rai, R. R. Tewari and S. K. Upadhyay, “Different Types of Attacks on Integrated MANET - Internet Communication,” International Journal of Computer Science and Security, Vol. 4, No. 3, 2010, pp. 265-274.

[3]. B. S. Sahu and K. Shandilya, “A Comprehensive Survey on Intrusion Detection in MANET”, International Journal of Information Technology and Knowledge Management, Vol.2, No. 2, pp. 305-310, 2010.

[4]. Sunil Taneja and Ashwani Kush “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285, August 2010.

[5]. Ipsita Panda “A Survey on Routing Protocols of MANETs by Using QoS Metrics” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012

[6]. Yu Zhang, Loukas Lazos and William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing (Article in Press), pp1-14, 2012.

[7]. Jordi Cucurull, Mikael Asplund, Simin Nadjm-Tehrani and Tiziano Santoro, "Surviving Attacks in Challenged Networks", IEEE Transactions On Dependable and Secure Computing, Vol. 9, No. 6, pp. 917-929 November/December 2012.

[8]. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu, "Risk-Aware Mitigation for MANET Routing Attacks", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, pp. 250-260, March/April 2012.

[9]. Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini,and Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks" IEEE Transactions on Mobile Computing, Vol. 12, No. 2,Pp. 289-303, February 2013.

[10]. S. Capkun, L. Buttyn, and J. P. Hubaux, “SECTOR: Secure tracking of node encounters in multi-hop wireless networks,” in 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 2003.

[11]. N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in ACM Workshop on Wireless Security (WiSe 2003), September 2003.
http://www.isi.edu/nsnam/ns/tutorial/index.html