International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 03 (MAY-JUN, 2016)

A Survey of Attacks Malicious Effects and Security in MANET

Aradhana Saxena
Computer Science
Gwalior Institute of Technology and Science, Gwalior, India
Saxena.aradhna@gmail.com

Prof. Mayuresh Kanhere
Computer Science
Gwalior Institute of Technology and Science, Gwalior, India
mayureshkanhere@gmail.com

***Abstract*—the number of nodes in wireless network is able to communicate with each other without any presence of physical medium. The nodes communication is possible by obtaining the signals from any medium like tower, modem etc. In Mobile Ad hoc Network (MANET) all the nodes are freely moves in the absence of without ant centralized coordination system. The attackers or malicious nodes are easily affected that kind of network and responsible for the routing misbehavior. The routing in network is mandatory to deliver data in between source and destination. One of the major challenges in Mobile Ad hoc Network face today is security. In this paper we proposed a profile based protection scheme (PPS security scheme against TRA (Traffic Remapping Attack). This kind of attacks are flooding access amount of unnecessary packets in network by that the network bandwidth are consumed by that data delivery in network are affected. The aim of previous work discussed in this paper is in presence of attack is to identify the attacker misbehavior or attackers that are affected the network performance. The particular security scheme are check the profile of each node in network and only the attacker is one that performing malicious activities. In this paper the whole survey of attacks, security scheme recent proposed by different authors and the short overview of routing protocols and MANET is also discussed. This survey provides the information about attackers and effect of traffic remapping attack is really harmful but does not lot of work is done in field of this attack.**

***Keywords*— MANET, Security Goal, PPS, TRA, Defensive mechanisms**

INTRODUCTION

Mobility and also the lack of any mounted infrastructure create Mobile Ad-hoc Networks (MANETs) terribly beautiful for brand spanking new age applications. There are many numerous problems and challenges in coming up with a MANET network like limited bandwidth, security and dynamic topology [1]. These nodes which are within each other's radio range can communicate directly, while distance nodes rely on their neighboring nodes to forward packets. In MANETS every node can be a host or router. Mobility, an advantage of wireless communication, gives a freedom of moving around while being connected to a network environment. Ad-hoc networks are so flexible that nodes can join and leave a network easily as compare to wired network [2]. Such networks can be used in the battlefield application, in disaster management and in remote areas where establishment and management of fixed network is not possible. These can also be used in the areas where the establishment of fixed infrastructure is very difficult. MANETs can also be used to deploy and coordinate the drones in the battle field. The set of applications for MANETs is miscellaneous, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. As Wireless networks have become increasingly popular in the past few decades, particularly within the 1990's when they are being adapted to enable mobility and wireless devices became popular. As the popularity of mobile devices (MDs) and wireless networks significantly increased over the past years, wireless ad hoc networks has now become one of the most lively and active fields of communication and networking research. As there are many attractive future applications of mobile ad hoc networks (MANETs), there are still some critical challenges and open problems to be solved. However, Mobile ad hoc, network the approach does not contain any fixed infrastructure. All nodes in a mobile ad hoc network can be dynamically connected to each other and are free to move. All nodes in the network are hosts and routers as well [1, 3]. Ad hoc networks usually have lower available resources compared with infrastructure networks and the highly dynamic nature of ad hoc networks means that many special factors have to be considered when designing a routing protocol specialized for them, such as network topology, routing path and routing overhead; also it must find a path quickly and efficiently.

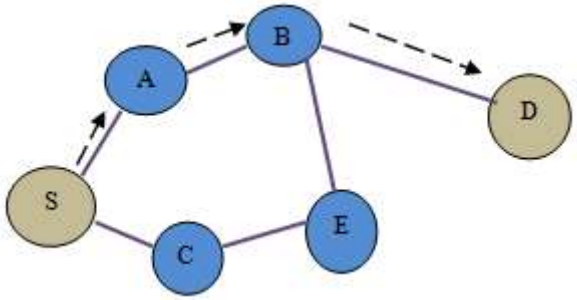

Figure 1 Communication between Nodes on MANETs

The transmission range of each node is limited in wireless ad hoc networks and thus not all nodes can directly communicate with each other. A node is often required to forward packets to another node to accomplish a communication across the network. An ad hoc routing protocol must dynamically establish and maintain routes between source and destination nodes for there is no static network topology and fixed routes. The sample diagram of mobile ad hoc network is depicted in figure 1. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure 1 (the dashed lines show the direct links between the nodes). If node

A moves out of node S' range, he has to find an alternative route to node D (S-C-E-B-D). A variety of new protocols have been developed for finding/updating routes and generally providing communication between end points (but no proposed protocol has been accepted as standard yet). However these new routing protocols, based on cooperation between nodes, are vulnerable to new forms of attacks.

Applications of MANET

The set of applications for MANET [4] is various, preparatory from large-scale, mobile, highly dynamic networks, to small, stationary networks that are anxious by power sources. Besides the inheritance applications that move from ancient infrastructure environment into the spontaneous context, a good deal of latest services can and {can} be generated for the new environment. Typical applications include:

1) Military section of ground: - Military equipment currently habitually contains some kind of laptop instrumentality. Ad hoc networking would permit the military to require advantage of commonplace network technology to take care of an information network between the soldiers, vehicles, and military information head quarters. The essential techniques of spontaneous network came from this field.
2) Business sector: - MANET may be utilized in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations should happen wherever non-existing or broken communication infrastructure and hasty preparation of a communication network is required. Information is relayed from one rescue team member to a different over a tiny low hand-held. Alternative business situations embrace e.g. ship-to-ship ad hoc mobile communication, enforcement, etc.
3) Local level: - Mobile Ad hoc Networks will autonomously link a rapid and temporary multimedia system network victimisation notebook computers or palmtop computers to spread and share information among participants in a conference or room. Another acceptable native level application may well be in home networks wherever devices will communicate on to exchange information. Equally in alternative civilian environments like car, structure, boat and little craft, mobile ad hoc communications can have several applications.
4) Personal space Network (PAN):- Short range MANET will simplify the communicating between numerous mobile devices (such as an organizer, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can even extend the access to the web or alternative networks by mechanisms e.g. Wireless computer network (WLAN), GPRS, and UMTS. The PAN is probably a promising application field of MANET within the future pervasive computing context.

Characteristics of MANET

All routers are mobile and might communicate with one another only if they're in transmission range. Second, ad hoc wirelesses nodes are resource strained, with restricted process and memory capability, and are typically powered with batteries. Finally, the communication medium in an ad hoc wireless network, i.e., radio waves, infrared, etc., can be simply eavesdropped. Hostile environments like battlefields or commando rescue operations are a number of the vital target application areas for Ad hoc wireless networks. We have a tendency to get the various forms of characteristics [5] of dynamic network.

1) Dynamic Network Topology:- This is triggered by node mobility, nodes effort or change of integrity the network, node inoperability as a result of the shortage of power resources, etc. still, the network connectivity ought to be maintained so as to permit applications and services to work undisrupted.
2) Limited Link Capacity:- The effects of high bit error rate are a lot of profound in wireless communication. over one end-to-end path will use a given link in ad hoc wireless networks, and if the link were to interrupt, might disrupt many sessions throughout amount of high bit transmission rate.
3) Distributed Operations:- The protocols and algorithms designed for an ad hoc wireless network ought to be distributed so as to accommodate a dynamic topology and an infrastructure less design. Wireless devices are battery powered, so there's a restricted time they will operate while not ever-changing or make full their energy resources. Coming up with energy economical mechanisms are so a crucial feature in coming up with algorithms and protocols.

TYPES OF ATTACKS IN MANET

The attacks in MANETS are classified into two major categories [6, 7], namely.

Passive Aattacks

Passive attacks are those, launched by the adversaries solely to snoop the data exchanged in the network. These adversaries in any way don't disturb the operation of the network. Such attacks identification becomes very difficult since network itself does not affected and they can reduced by using powerful encryption techniques.

Active Attacks

The active attack tries to alter or destroy the information that is being exchanged, thereby disturbing the normal functionality of the network. In MANET malicious and undesirable nodes to disrupted the normal functioning in the network. Some of the common attacks [7, 8] in MANET are as follows:-

1) 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.
2) Wormhole Attack:- The main aim of the wormhole attack is to replay the packet on the other side of the network. This

attack is executed by two nodes colluding to form a wormhole. The attacker on one side make the nodes believe that distance to the destination is just one hop, when it is greater than one hop. This causes the attacker to attract all the traffic from one side of the network and relay it through the wormhole; the attacker on the other side replays the same packet. By doing this the attacker can drop the packets or obtain any service illegally.

3) Denial Of Service (DoS) Attack and Flooding:- The aim of this attack is to cripple the smooth functioning of the network. This attack is accomplished by continually sending packets into the network causing the targeted node in the network to process them and keep them occupied resulting in the crashing of that node. By executing this attack, the attacker keeps the targeted node busy in processing its fabricated packets and depriving the legitimate RREQs to be dropped. This attack can cause the network infrastructure to collapse.
4) Sybil Attack:- In the Sybil attack [9], an attacker pretends to have multiple identities. A malicious node can behaves as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Sybil attacks are classified into three categories like direct or indirect communication, fabricated or stolen identity, and simultaneity. In the direct communication, Sybil nodes communicate directly with legitimate nodes, whereas in the indirect communication messages sent to Sybil nodes are routed through malicious nodes. An attacker can fabricate a new identity or it can simply steal it after destroying or temporarily disabling the impersonated node. All Sybil identities can participate simultaneously in the network or they may be cycled through.
5) Byzantine attack: :- In a Byzantine attack [10] compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.
6) Rushing attack::- In rushing attack [6, 11] an attacker takes the RREQ packet from source node floods the packet quickly to all the other nodes in the network, before they get the same packet from the source. Once the original RREQ packet comes to the nodes, they assume it is a duplicate one and rejects it since they already have the packet from adversary.
7) Remapping attack: - The remapping attack [20] is similar to DoS attack i.e. huge numbers of packets are flooded by attacker in network. The difference is that in remapping attack the attacker is shown their communication is on first priority and this priority is actually of any other sender in network. The priority level is decided randomly and also possible to select attacker but attacker is not shown sender at that instant because it grasp the higher priority of sender for flooding misbehavior in MANET.

ROUTING PROTOCOL OVERVIEW

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [13]. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also routers that route data to/from other nodes in network [2].

Proactive Routing Protocols

Proactive protocols like Destination Sequenced Distance Vector (DSDV) [13, 14], Optimized Link State Routing (OLSR) [15] continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. If the network topology changes too frequently, the cost of maintaining the network might be very high. If the network activity is low, the information about actual topology might even not be used.

Reactive Routing Protocols

The reactive routing protocols Dynamic Source Routing protocol (DSR) [16], Ad Hoc on Demand Distance Vector protocol (AODV) [17], Temporally Ordered Routing Protocol (TORA) [18] are based on some sort of query-reply dialog. Reactive protocols proceed for establishing route(s) to the destination only when the need arises. They do not need periodic transmission of topological information of the network.

Hybrid Routing protocol

Often reactive or proactive feature of a particular routing protocol might not be enough instead a mixture might yield better solution. Hence, in the recent days, several hybrid protocols are also proposed like ZRP [19].

RELATED WORK

This section presents related work about existing work done in the field of MANET routing protocol, congestion control. Jerzy Konorski and Szymon Szott, [20] “Discouraging Traffic Remapping Attacks in Local Ad Hoc Networks” we discuss in this topic **a** distributed discouragement scheme based on the threat of TRA detection and punishment. The scheme does not rely on station identities or a trusted third party, nor does it require tampering with the MAC protocol. We analyze an arising non-cooperative TRA game and find that under certain realistic assumptions it only incentivizes TRAs if they are harmless to other stations; otherwise the selfish stations are induced to learn that TRAs are counterproductive. Sevil Sen,, John A. Clark [21] “Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks” In this title we explore the use of evolutionary computation techniques, particularly genetic programming and grammatical evolution, to evolve intrusion detection programs for such challenging environments. Cognizant of the particular importance of power

efficiency we analyze the power consumption of evolved programs and employ a multi-objective evolutionary algorithm to discover optimal trade-offs between intrusion detection ability and power consumption. In this paper [22] three routing algorithms are presented namely disjoint multipath routing (DMR), Trust based multipath routing (TMR), and message trust based multipath routing (MTMR). All the three routing protocols have their own way in order to establish the trust and transmit packet securely. The performance metric considered are, number of hops, route discovery time and packet loss, The simulation results show that MTMR protocol works much better and provides less number of hops, less route discovery time and less packet loss. This paper [23] proposes a secured message security scheme for MANETs (our so-called T-AOMDV) that uses a trust-based multipath AOMDV routing combined with a soft-encryption methodology to securely transfer messages. More precisely, our approach consists of three steps: (1) Message encryption: where at the source node, the message is segmented into three parts and these parts are encrypted using one another using some XOR operations, (2) Message routing: where the message parts are routed separately through different trust based multiple paths using a novel node disjoint AOMDV protocol, and (3) Message decryption: where the destination node decrypts the message parts to recover the original message. In this paper [24], we have proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent black hole attacks imposed by both single and multiple black hole nodes. Result of a simulation study proves the particular solution maximizes network performance by minimizing generation of control (routing) packets as well as effectively preventing black hole attacks against mobile ad-hoc networks. P. Raj and P. Swadas [25], proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast. In this paper [26], we present a method to securely route messages in an ad-hoc network using the concepts of multipath routing and trustworthiness of the nodes. We divide the message into different parts and encrypt these parts using one another [27]. We then route these parts separately using different paths. An intermediate node can access different parts on the basis of its trustworthiness. In other words, a more trusted node is allowed to feature in more paths than a less trusted node and hence has access to more message parts than a less trusted node. This feature allows the routing algorithm to avoid nodes that are more likely to attempt 'breaking-in' the encryption. In addition, suspected nodes, which have high computation power and are hence likely to be more successful in cryptanalysis, can be given less parts to stymie their plans. In this paper [28], proposed an approach that tackles with particularly the network layer attacks. We detect nodes that misbehave by launching attacks on either a single node or parallel to more number of nodes by inducing significant delay in the packet or by altering the contents of the packets or by routing the packet to a non-destined node or by sending a packet out of transmission range or some other means. The proposed scheme uses one way hash computation which is highly impossible to be known by the malicious nodes to launch an attack. The core idea of this algorithm is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. In this paper [29], we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing [17] for analysis of the effect of the black hole attack when the destination sequence number is changed via simulation. Then, we select features in order to define the normal state from the characteristic of black hole attack. Proposed training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment. Authors [30] "An Efficient Mechanism of Handling MANET Routing Attacks using Risk Aware Mitigation with Distributed Node Control" In this title, we discuss a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

CONCLUSION AND FUTURE WORK

The mobile nodes in MANET are forming the dynamic link that is periodically changes in the absence of internal coordination system and also because of that security is the major issue in MANET. The data packets in network are delivering in between sender and receiver through routing mechanism of connection establishment. In MANET attacker of malicious nodes are easily affected the routing performance of network. The attackers are dropping the all data packets that are the reason of routing misbehavior in MANET. But the flexibility of decentralized administration in mobile nodes communication provides the results in a dynamic topology, that makes it very difficult in developing secure ad-hoc routing protocols. The radio channel used for ad hoc networks is broadcast in nature and is shared by all the nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So attackers can easily affect the data being transmitted in the network. This survey is provides the information of different attacks and their effect in dynamic environment. The different attackers has different strategy to performing misbehavior like black hole is dropped, wormhole is making tunnel and remapping attack is change the priority of communication but their aim is only one

to destroy the network performance in MANET. Ad hoc networks are vulnerable due to their structure less property. A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. Due to highly dynamic topology change MANET is attract researchers for more development. In further from research point of view, it is possible to develop a new security scheme in MANET. As per literature review it is analyzed that various security schemes are developed in MANET however not a single one technique is fully efficient especially for remapping attack.

REFERENCES

[1] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), pp. 13–6, 2003.

[2] M. Conti, S. Giordano "Multihop ad hoc networking: The Theory", IEEE Communication Magazine, 2007.

[3] Basagni, S., Conti, M., Giordano S., and Stojmenovic, I. (Eds.) Ad Hoc Networking. IEEE Press Wiley, 2003.

[4] Saleh Ali K.Al-Omari, Putra Sumari, "An overview of mobile ad-hoc network for the existing protocol and application", International Journal on Application of Graph Theory in Wireless Ad hoc Network and Sensor Network.Vol2,No.1,March 2010.

[5] Seema Dev D. Aksatha D, T. Lalitha, "Comprehensive Overview on Manet", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3 Issue-6, August 2014.

[6] Satyam Shrivastava, Sonali Jain, A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network" International Journal of Computer Science & Engineering Technology Vol. 4 No. 03 March 2013.

[7] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks", Proceeding of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004.

[8] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) pp. 265-274, 2010.

[9] Abu Taha Zamani, Javed Ahmad, "A Novel Approach to Security in Mobile Ad Hoc Networks (MANETs)", International Journal of Computer Science and Information Technology Research, Vol. 2, Issue 1, pp. 8-17, January-March 2014.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," presented at the 3rd Int. Symposium Information Processing in Sensor Networks (IPSN), 2004.

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[12] Y. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Proceeding of the ACM Workshop on Wireless Security (WiSe), pp. 30-40, 2003.

[13] Laura Marie Feeney, "A Taxonomy For Routing Protocols in Mobile Ad Hoc Networks, Technical report, Swedish Institute of Computer Science, Sweden, 1999.

[14] Krishna Gorantala, "Routing in Mobile Ad-hoc Networks", Umea University, Sweden, June-2006.

[15] T. Clausen, et. al, "Optimized Link State Routing Protocol", Internet Draft: draft ietf- manet-olsr- 05.txt, October, 2001.

[16] D.B. Johnson, D. A. Maltz and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet Draft: draft-ietf-manet-dsr-06.txt, November 2001.

[17] C. E. Perkins, E. M. Royer and S.R. Das, "Ad hoc On-Demand Distance Vector Routing," Internet Draft: draft-ietf-manet-aodv-09.txt, November 2001.

[18] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA) Version1 Functional Specification," Internet Draft: draft-ietf-manet-tora-spec-04.txt, 2001.

[19] Z. Hass, and M. Pearlman, "The performance of query control scheme for the zone routing protocol", in Proceeding of ACM SIGCOMM, August 1998.

[20] Jerzy Konorski and Szymon Szott, "Discouraging Traffic Remapping Attacks in Local Ad Hoc Networks" IEEE Transactions On Wireless Communications, Vol. 13, No. 7, July 2014.

[21] Sevil Sen, John A. Clark "Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks" Computer Networks May 10, 2011.

[22] Dd Mohana, N.K. Srinath, Amit L.K, "Trust Based Routing Algorithms for Mobile Ad-hoc Network International Journal of Emerging Technology and Advanced Engineering (IJETAE)", Volume 2, Issue 8, pp. 218-224, August 2012.

[23] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher, " Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks" IEEE Globecom 2011 proceedings.

[24] Yibeltal Fantahun Alem Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" IEEE 2nd International Conference on Future Computer and Communication (ICFCC), pp.V3-672 - V3-676, 21 to 24 MAY 2010.

[25] P. Raj and P. Swadas, "A dynamic learning system against black hole attack in AODV based MANET,"

IJCSI International Journal of Computer Science, Vol. 2, pp. 54-59, 2009.

[26] Prayag Narula, Sanjay Kumar Dhurandher, Sudip Mira, Isaac Woungang, " Message Security in Mobile Ad-Hoc Networks: Using Trust-Based Multi-Path Routing Approach" IEEE International Conference on Computer Engineering & Systems (ICCES '07), 2007.

[27] Haniotakis, T., Tragoudas, S. and Kalapodas, C., "Security Enhancement through Multiple Path Transmission in Ad Hoc Networks", In Proceedings of IEEE International Conference on Communications, pp. 4187-4191, June 2004.

[28] G.S. Mamatha and Dr. S. C. Sharma "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, 1793-8201, October, 2010.

[29] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto, " Detecting Black hole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[30] Sk. Rahima Sulthana, D. Srujan Chandra Reddy, T. Bharath Manohar "An Efficient Mechanism of Handling MANET Routing Attacks using Risk Aware Mitigation with Distributed Node Control" International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 5, Sep - October 2013 pp-2996-3004.