Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

The IDS for Securing MANET from Packet Dropping Attack

Ghanshyam Rathore
Computer Science & Engg. Dept.
Indore Institute of Science and Technology
Indore,India

Prof. Ranjeet Osari
Computer Science & Engg. Dept.
Indore Institute of Science and Technology
Indore,India

***Abstract*—This work analyzes the effect of packet dropping attack through malicious nodes which is probable attacks in ad hoc networks. In this attack, a malevolent node or malicious node impersonates a target node by sending a spoofed route reply packet to a source node which initiates a route discovery. MANET may be unprotected against attacks by the malicious nodes. One of these attacks is the packet dropping Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination by that due to this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this paper we proposed a simple IDS Algorithm against dropping attack and measure the network performance after applying IDS. We simulated dropping attacks in network simulator 2 (ns-2) and measured the packet loss in the presence of attacker and in presence of Intrusion Detection System against malicious attack. proposed solution improved the 80% network performance in the presence of a packer dropping attacker.**

Keywords:- Packet Dropping Attack, IDS, Routing, AODV, Security

I. INTRODUCTION

The wireless medium has become the newest trend in today's world for data communication. MANET also uses wireless medium for data communication. A Mobile Ad hoc Network (MANET) is the system of infrastructure less or wireless mobile nodes that dynamically constructed in arbitrary and temporary network topologies [1, 2]. Mobile ad hoc networks (MANET) are collection of wireless networks, which consists of huge number of mobile nodes. Nodes in Mobile Ad hoc networks (MANET) can connect and leave the network dynamically. The mobility and scalability of MANET which does not require any fixed network infrastructure, makes it popular for different applications. So, it is very useful for emergency situation like military operation or disaster management [3,4]. By definition, MANET is a collection of mobile nodes equipped with the both wireless transmitter and a receiver which communicate with each other via bidirectional link directly or indirectly. MANET is an autonomous, self configuring network. This network can be deployed anywhere with ease without no support on any fixed infrastructure. There is infrastructure less and centralized administration in this type of networks. Nodes are constant from first to last wireless interface. The dynamic nature of such type of networks makes it highly strung to various link attacks. The essential requirements for a secured wireless networking are secure protocols which certify the discretion, availability, validity, truth of network [5,6]. Many existing safety solutions for wire oriented networks are inefficacious and inefficient for Mobile ad hoc networks (MANET) environment. An ad hoc network is the co-operative environment of a system of mobile nodes which does not required an obstruction of any centralized system. An ad-hoc network is the temporarily established and created network, which is managed and operated by participating nodes. A mobile **S** sender S node forming a temporary connection in through intermediate nodes to destination **D**. The node **C** is out of range to next node due to that the link from that is not possible.

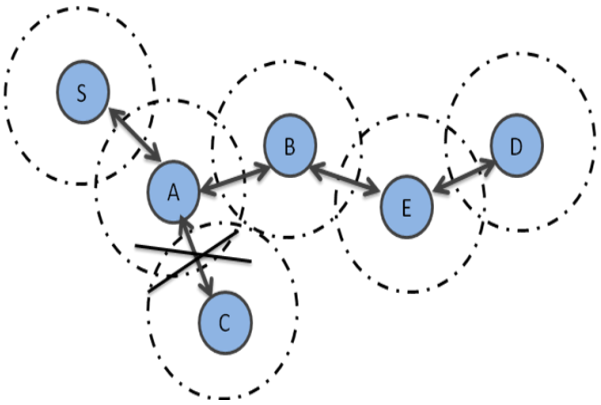


Figure1 Ad hoc network

Mobile ad hoc network (MANET) is a group or set of mobile nodes which can contact to each other by using multi-hop wireless links. Mobile ad hoc network does not require any centralized management system and fixed network topology of nodes. Mobile ad hoc network is spontaneous, infrastructure or topology less and self organized network. MANET has wide area use because of their self establishment, self creation and self maintenance. Mobile ad hoc network (MANET) is an important part for communication for mobile system. Mobile system or nodes or device in the mobile ad hoc network has a freedom for entry or exit from the network. Mobility reflects the frequently change of network topology. Mobile nodes in the mobile ad hoc network which has the same communication range are said to be the neighboring nodes and neighboring nodes can contact directly to each other. Mobile nodes in MANET can communicate to each other by passing the data and control packets from one node to another node, which are in the same wireless range. Trusted and co-operative behavior of mobile nodes helps in the communication of mobile nodes in the MANET. The mobile

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

nodes in a MANET may be laptop, router, cell phone, personal digital assistants etc. Mobile Nodes establishes the virtual group of connection which helps to each other in passing information and control packets to each other.

II. Literature Survey

In this paper [7], we develop an exact algorithm for detecting selective packet drops which made by a insider attackers. The given algorithm also bestows a truthful and publicly provable decision statistics as authenticate to support the detection decision. The basic approach in this paper is that even though malicious dropping may result in a packet loss rate that is comparable to the normal channel losses, the stochastic processes that explain the two phenomena exhibit the different correlation structures (equivalently, different patterns of packet losses). hence, by detecting the correlations between the lost packets, one can decide whether the packet loss is purely due to regular link errors, or due to a combined effect of the link error and malicious drop. The proposed algorithm in this paper takes into account the cross-statistics between lost packets to compose a more informative decision, and therefore is in sharp contrast to the conventional methods that confide only on the distribution of the number of lost packets.

In this research [8] the author mainly focuses on improving the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to protect it against flooding attacks and black hole attacks. The performance analysis of this research carried out shows betterment in packet delivery ratio in presence of the black hole attack, with marginal rise in average end-to-end delay and the normalized routing overhead. The proposed mechanism for the flooding attack works even when the malicious nodes is unidentified and does not use any additional network bandwidth. It is easy to implement and maintains or improves the network throughput when there are no malicious nodes present but the network is congested with excess traffic.

In this paper [9] the author proposed a hierarchical dynamic trust management protocol for the cluster-based wireless sensor networks that is consider the two aspects of trustworthiness, namely, social trust and the QoS trust. they developed a probability model utilizing stochastic Petri nets techniques to explore the performance of the protocol, and validated subjective trust against the objective trust that is obtained based on ground truth node status. They demonstrated the possibility of dynamic hierarchical trust management system and application-level trust optimization design concepts with the trust based geographic routing and trust-based IDS applications, by recognizing the best way to form the trust as well as use trust out of individual social trust and QoS trust properties at the runtime to improvement the application performance. In this research, the trust-based IDS algorithms outmatch the traditional anomaly-based IDS (intrusion detection system) techniques in the detection probability while maintaining sufficiently low false positives.

In this paper [10], The authors discuss the different types of security attacks that can be launched in easy way in MANETs and related solutions is very needful for ensuring the network security in the wireless network. There is the implementation of the SAODV (secure ad hoc on-demand distance vector routing protocol) and compares the performance of protocol with existing AODV protocol in the presence of black hole attack in this paper. Since public key cryptography is used in this methodology, it obtains the significant amount of time to compute the digital signature at each node. Also, this leads to the high overhead and processing power necessities.

In this paper, author proposed the term "FACES" (Friend-Based Ad-hoc Routing using Challenges to Establish Security) [11], that is providing a list of trusted nodes to the source node by sending some challenges and sharing friend lists in the network. That list is based on the range of successful data transmission and the friendship with any other nodes in a network; the nodes that are presented in the friend lists, are rated. The trust level of each node varies from -1 to 4. The nodes are placed in one of the three lists in the network, i.e. question Mark list, friend list and unauthenticated list. The periodic flooding attack of challenge packets and sharing of friend lists increases the control overhead.

III. Proposed Work

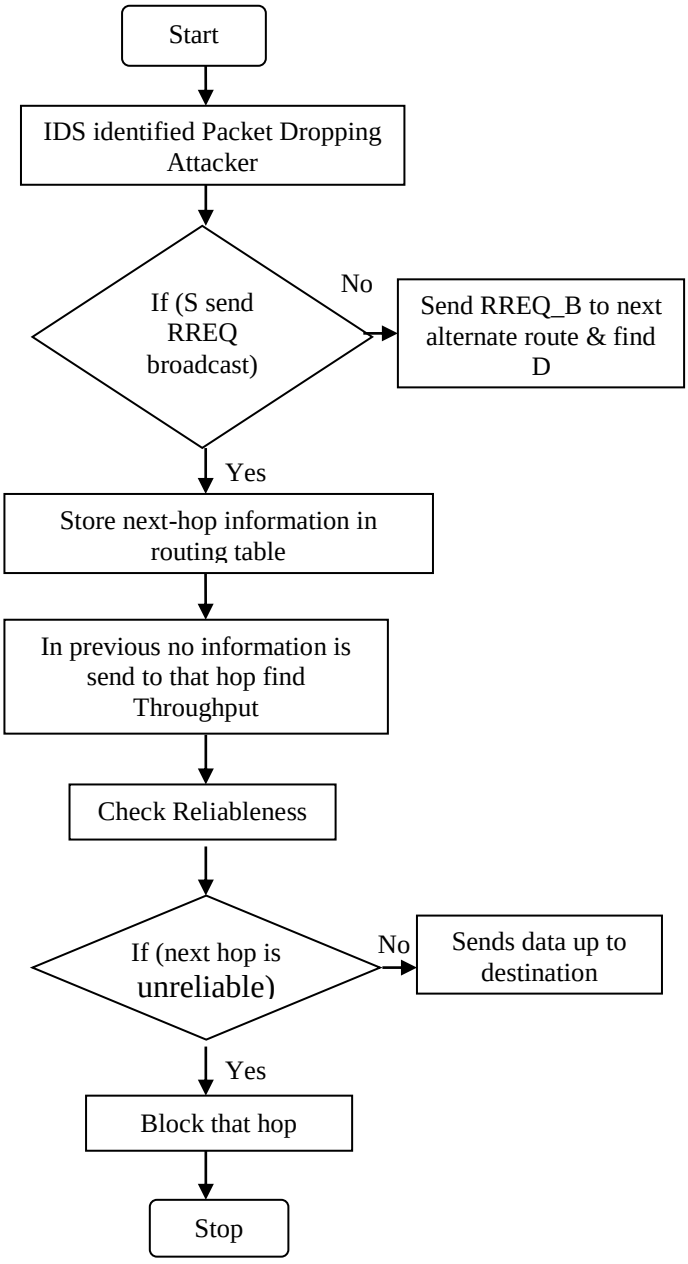
The Every packet in MANETs contains a distinctive sequence number. This number is an increasing value, i.e., consequent packet should have higher value that the present packet sequence number. The node in regular routing protocols contains the last packet sequence range that it's received and uses it to examine if the received packet was received before from identical originating source or not.

In Intrusion detection system (IDS), each node must have two extra small-sized tables; one to stay last-packet-sequence-numbers for the last packet sent {to each|to each} node and also the different to stay last-packet-sequence-numbers for the last packet received from every node (from node through node). These tables are updated once any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it'll initiate a RREP to the supply, and this RREP can contain the last- packet-sequence-number, that is received from this source. Once an intermediate node contains a route to the destination and receives this RREQ, it'll reply to sender with a RREP contains the last-packet-sequence-numbers received from the source by this intermediary node. This solution gives quick and reliable thanks to determine the suspicious reply. No overhead are going to be additional to the channel as a result of the sequence range itself is enclosed in each packet within the base protocol.

Every packet in MANETs features a distinctive sequence range. This range is associate increasing worth, i.e., successive packet should have higher worth that this packet sequence range. The node in regular routing protocols keeps the last packet sequence range that it's received and uses it to envision if the received packet was received before from identical originating supply or not.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

Flow Chart



The steps to known attack

```
The IDS are known the packet dropping attacker.
{
 If ( S send RREQ_B) // { S is the sender and D is the
destination
{
Additional filed to rtable (next_hop , Through)
Known in previous No information through that hop;
However exist in rtable enetry ; //Check reliableness
  if next hop (next_hop is unrelaible);
        {
        Block that Hop ;
        }
        else
        {
        until the Destination;
        }
 Else
Send_RREQ_B to next alternative hop ;
Search destination D;
        }
}
```

IV. Simulator Overview

The NS-2 (Network Simulator) is the discrete event driven simulator used for implementation and the simulations of the various network protocols. It is freely distributed, open source and is widely used for the research.

NS-2 is also provide infrastructure for tracing, visualization, error models, etc. and to modify or creates your own modules. Using components in ns, many traffic and topologies can be generated and NAM (Network Animator) can be used for visual outputs.

Network simulator is the open source event driven simulator, which is basically design for simulating the communication networks such as wire oriented network, wireless ad hoc network and wireless sensor network. NS-2 (Network Simulator) contains the various module for the network such as routing, application layer protocol, transport layer protocol. Performance of network can be evaluated by researchers by configuring the network in any scripting language such as tcl and Otcl. They can get the result created by NS2. NS2 is a network simulator that is open source available, described by T and it has wide area used. Network Simulator is a tool which contains various packages that are used for simulating the behaviour of the network.

A. Performance evaluation parameters

We evaluate the performance of AODV protocol in the Security Scheme against packet Dropping attack on the following four performance parameters:

1. Throughput: Throughput is defined as the measure of how fast we can really send packets through network. The number of packets which are delivered to the receiver provide the throughput of the network.

2. Packet Delivery Ratio (PDR): Packet Delivery Ratio (PDR) is the ratio of data packets delivered to the destinations to those generated by the CBR sources.

3. Packets dropped: it represents some of the packets generated by the source; those packets will get dropped in the network cause of high mobility of the nodes, congestion of network etc.

4. Normalized routing overhead: Normalized routing overhead is described as the number of routing packets transmitted per data packet delivered at the destination end. Each hop-wise transmission of a routing packet is counted as one transmission in network.

V. RESULT ANALYSIS

A. Packet Delivery Ratio Analysis

Packet Delivery Ratio is the percentage of packets received at destination in a given simulation time of 100 seconds. The PDR of attack at start is about 25 % at time 2 second and up to 22 seconds but after that 2% up to time 90 seconds, after that again reaches to 25%. The Performance of Secure is better to Normal routing performance i.e. more than 95%.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

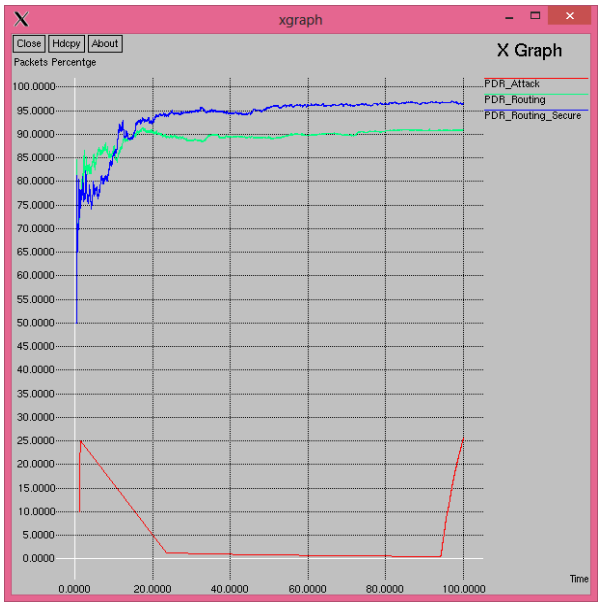


Figure 1 PDR Analysis

B. Routing Load Analysis

Routing Load Analysis of the network is define as, it is measured as the number of routing packets transmitted for the each data packet delivered at the destination. The Routing Load in the Normal status is about the 6900 data packets communicate at the time 99 seconds and when a malicious node is present in the network then only 1495 data packets communicate and when we applied our scheme means at the Secure status, there are about 2500 data packets are communicate in 100 seconds. In the routing load analysis of Secure is better than both normal and Malicious because the load of 6900 has no sense and at malicious only 1495 data Packets communicate in 99 seconds means performance is very low. So we can say our secure scheme is better than other.

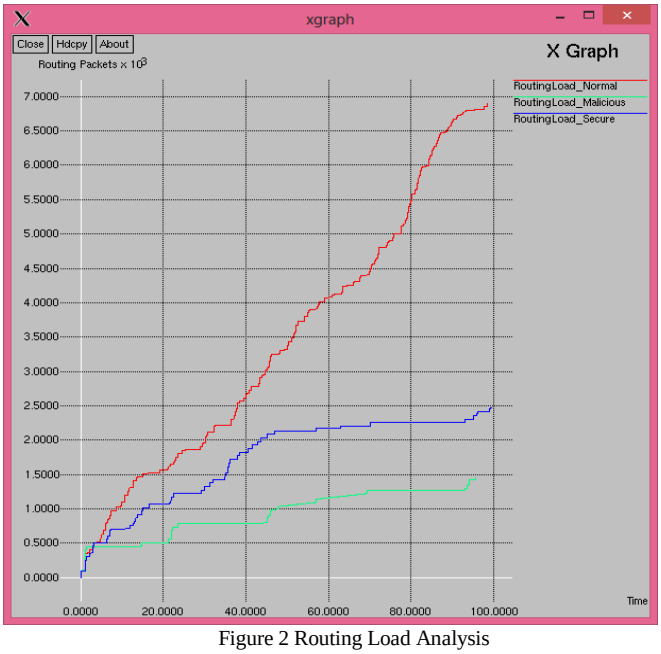


Figure 2 Routing Load Analysis

C. Throughput Analysis

Throughput analysis shows the total number of data packets send in per unit of time. At the normal stage as the figure shows in normal at the start packets are growing up at the time about 46 seconds approximate 600 and up to at time 90 seconds only 370 packets remaining and same as at malicious there is about the 170 packets at starting time and up to 21 seconds there is no packets while in secure at the start the packets are grow up up to the about 620 packets at time about 100 Seconds. So our approach is better than both.

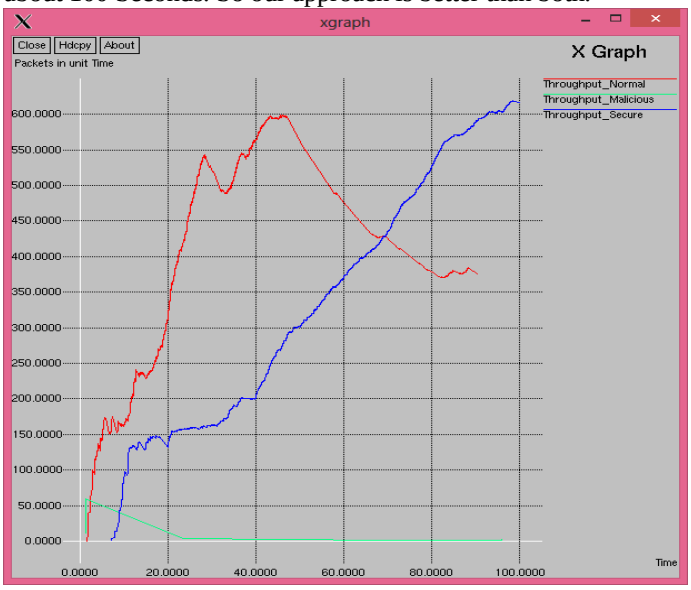


Figure 3 Throughput Analysis

D. UDP Received Analysis

UDP Received analysis shows the total number of data packets received at per unit of time. At the normal stage as the figure shows in normal at the start packets there is 525 are received at time about 87 seconds up to 100 seconds and same as at malicious there is no packets received till the end of time and while in secure approximate 860 packets are received in 100 seconds So our approach is better than both.

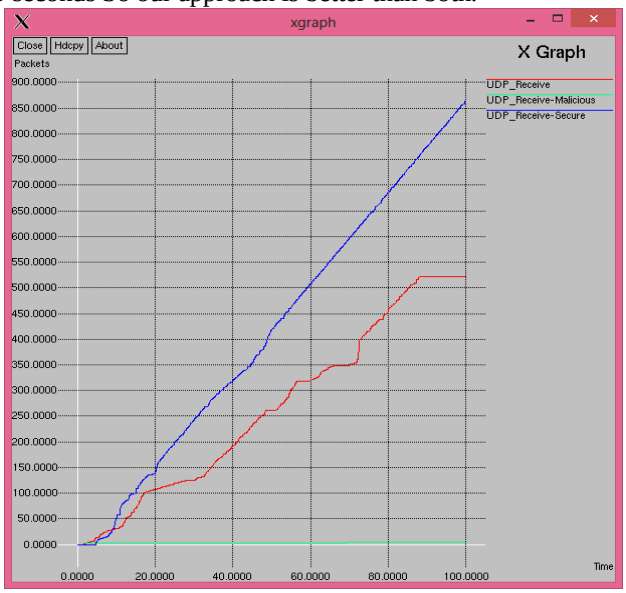


Figure 4 UDP Received Analysis

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

E. Complete Performance Analysis of Normal, Malicious and Secure

The Complete Comparative Performance Analysis at Normal mode, Malicious Mode and at Secure Mode are shown in following Table 1

Performance		Normal	Malicious	Security
SEND	=	7330	1838	6023
RECV	=	6663	469	5810
ROUTINGPKTS	=	6894	1456	2467
PDF	=	90.9	25.52	96.46
NRL	=	1.03	3.1	0.42
Hop Count	=	1423	4985	143
Average e-e delay(ms)	=	491.76	118.84	660.41
No. of dropped data (packets	=	667	1369	213

Table 1 Complete Analysis of Normal, Malicious and Secure Routing

Attacker Node	Loss of Data
15	294
36	375
37	291
38	209

Table 2 Attacker Detection and Packet Loss

VI. Conclusion and Future Work

The security is essential for this kind of decentralized network. In this research we simulate the scenario of attack, security and normal routing in networks and find its affects. In our study, we used the AODV routing protocol. But the other various routing protocols could be simulated also. In this synopsis, we try to resolve cooperative effect in the network. But the detection of the packer dropping attack is possible through proposed IDS security scheme. Our solution looks the path in the AODV level. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Effect on packet loss is clearly visualized in throughput and other metrics. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Its detection is the main matter of concern. Therefore the proposed IDS algorithm work will be excellent to detect and defense the network from malicious attack. Improvement for overcoming the effect of attack should orient towards controlling the delay.

The other attacker like wormhole is also dropping the packets by making the tunnel. In future some techniques should be proposed for reducing end to end delay. Also attackers like packet dropping and wormhole for AODV routing algorithm can be implemented in real life scenario and its analysis can be compared with the analysis results.

References

[1] Priyanka Goyal, sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks" International Journal of Computer Applications Volume 9– No.12, November 2010.
[2] Kisung Kim and Sehun Kim, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks".
[3] Ad hoc network specific attacks held by Adam Burg.
[4] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.
[5] C.K.Toh , "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Englewood Cliff, NJ 07632, 2002
[6] M. UmaparvathiDharmishtan K. Varughese "Two Tier Secure AODV against Black Hole Attack in MANETs" European Journal of Scientific Research.
[7] Tao Shu And Marwan Krunz,"Privacy-Preserving And Truthful Detection Of Packet Dropping Attacks In Wireless Ad Hoc Networks" IEEE Transactions On Mobile Computing, Vol. 14, No. 4, April 2015, 813-828.
[8] Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", 2012 International Conference on Computer Communication and Informatics (*ICCCI* - 2012), Jan. 10 – 12, 2012, Coimbatore, INDIA.
[9] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection IEEE Transactions On Network And Service Management, Pp. 169-182, Vol. 9, No. 2, June 2012
[10] Preeti Sachan, Pabitra Mohan Khilar, "Security Attacks and Solutions in MANET", Proceedings of International Conference on Advances in Computer Engineering, 011ACEEE, pp 172-176
[11] Pravina Dhurandher, "FACES: Friend Based Ad hoc Routing Using Challenges to establish security in MANET Systems" IEEE SYSTEMS Journal ,Volume 5, No 2, June 2011,pp:176- 188.
[12] K Fall and K. Varadhan, The NS Manual, November 18, 2010, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf. 2010.