International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Identification of Jamming Attack to Secure Decentralized MANET

Ashwini Magardey*& Dr. Tripti Arjariya**

[*] M. Tech Scholar, Department of Computer Science, Bhabha Engineering Research Institute, RGPV, Bhopal.

***Head, Department of Computer Science Engineering, Bhabha Engineering Research Institute, Bhopal, India.*

ABSTRACT:

Mobile Ad hoc Network (MANET) are typically created without any major infrastructure and centralized authority. It implies that, MANET is relatively vulnerable to malicious network attacks, and therefore, security is a more significant issue than infrastructure based wireless networks. In MANET, it is difficult to identify malicious hosts as the topology of the network dynamically changes. A malicious host can easily interrupt a route for which it is one of the forming nodes in the communication path. Since the topology of a MANET dynamically changes, the mere use of a static baseline profile is not efficient. In this paper we proposed the security scheme against jamming attack. The jammer node consumes the bandwidth capacity and proposed scheme is identified the jammer node that floods unwanted packets that are consumes the whole channel capacity in network. The proposed IDS (Intrusion Detection System) security scheme is identified the attacker by their routing profile of other nodes. The attacker has dump the whole performing of network. The Multipath routing protocol AOMDV is provides the multiple path if the attacker is exist in established path. The infection from attack and End to End connection performance is evaluated and observe the secure proposed security scheme is block the routing misbehavior and provides secure routing.

Index Terms—Multipath routing, Jamming attack, Security, IDS, decentralized, MANET,

I. INTRODUCTION

All Mobile ad hoc network (MANET) is formed by a set of mobile hosts which communicate among themselves by means of the air. Those hosts establish dynamically the network without relying on a support infrastructure and cooperate to forward data in a multi-hop fashion without a central administration [1]. MANETs were initially proposed for military applications and currently their use has been enlarged. Examples of application include emergency disaster relief, military battle field communication, sensing or controlling a region, sharing information during a lecture or conference, and so on [1]. Due to solution restrictions and MANET characteristics, researchers have focused on designing security mechanisms for achieving network survivability. Survivability is commonly defined as the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accident [2]. The term system has a wide sense and could characterize networks, means of communication or services, and mission represents the abstract goals and requirements of the system.

MANETs are susceptible to many security issues. Characteristics as dynamic topology, resource constraint, limited physical security and no centralized infrastructure make those networks vulnerable to passive and active attacks [3]. In passive attacks, packets containing secret information might be eavesdropped, violating the confidentiality principle. Active attacks include injecting packets to invalid destinations, deleting packets, modifying the content of packets, and impersonating other nodes. Because the network topology of MANETs frequently changes, and there is no central management entity, all of the routing operations must be performed by the individual nodes in a collaborative fashion. Consequently, it is unrealistic to introduce an authentication server that can employ conformist security schemes to secure the network against attacks from malicious hosts. The typical types of attacks in MANETs include eavesdropping, address spoofing, forged packets, denial of service (DoS), etc. [3].

MANET routing is considered as one of the most essential issues that need a scalable method because the network topology and transmitting data may become a requirement according to time. Routing is classified into two main categories: proactive routing and on-demand or single-path routing and multi-path routing [4]. The nodes in the network having a limited buffer space that causes the problem to handled heavy load in network. If the traffic is not distributed evenly, then some areas in a network are under heavy load while some are lightly loaded or idle.

Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network's capacity to perform its expected function" [5]. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information. In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication in network.

In this paper, we propose a new jamming attack detection and prevention IDS scheme based on a flooding identification method. The MANET hosts are mobile on their own so that the MANET environment is dynamically changing. Our proposed scheme is identified the packets flooding that provides the information of attacker and nodes that receives the jammer packets in network. The testimony details of routing misbehavior are entered in infected node routing table. The details of flooding packets detained the attacker and security scheme is block their misbehavior activities.

II. SECURITY CHALLENGES AGAINST ATTACK

A number of challenges remain in the area of securing Mobile Ad hoc Networks. First, the secure routing problem in such networks isn't well modeled. A more complete model of possible attacks would let protocol designers evaluate the security of their routing protocol to protect from routing misbehavior. In addition, such a model would form the basis for using

formal methods to verify protocol security. Another problem is designing efficient routing protocols that have both strong security and high network performance. Communities obviously rely on the trustworthiness of their members for their security and such mutual trust must be guaranteed throughout their existence.

In the same way as a majority of attacks against wired networks originate from within it, it is to fear that attacks from inside a community will not be rare. A mechanism should therefore assure that all the nodes in a community behave according to the security policy and deserve to be trusted. Moreover, we have seen that a mechanism such as routing performs best if it can rely on the cooperation of as many hosts as possible. In the case of a community evolving in an open environment containing unknown nodes this would most certainly lead to relying on strangers for data exchanges. The community should thus try to detect malicious nodes so as to exclude them when performing cooperative actions. Existing mechanisms, implemented through the use of communities, can only provide a certain security to ad hoc networks. Complementarily to these mechanisms mentioned in section 5, we feel that intrusion detection must be implemented to obtain an optimal security level in such networks. After going through an overview of existing solutions to intrusion detection and pointing out the requirements in the ad hoc context, we will propose a suitable IDS security scheme for such wireless, mobile environments. Although researchers have designed security extensions for several existing protocols, many of these extensions remove important performance optimizations. Optimistic approaches can provide a better tradeoff between security and performance.

III. BRIEF HISTORY OF JAMMING

The first occasions of jamming attacks were recorded back in the beginning of the 20th century against military radio telegraphs. Germany and Russia were the first to engage in jamming. The jamming signal most frequently consisted of co-channel characters.

The first wartime jamming activities can be traced back to the World War II [6], when allied ground radio operators attempted to mislead pilots by giving false instructions in their own language (an example of deceptive jamming). These operators were known by the code name ‘Raven’ which soon became ‘Crow’. The crow represents the universal sign of jamming ever since. Also during World War II the first jamming operations against radars (a new invention at that time) have been reported.

Jamming of foreign radio broadcast stations has been often used during periods of tense international relations and wartime to prevent the listening of radio broadcasts from enemy countries [7]. This type of jamming could be relative easy addressed by the stations with the change of transmitting frequency, adding of additional frequencies and by increasing transmission power. The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route takeover. There are some attacks against routing that have been studied are:-

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.

- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages.

A. Communication Protocol Stack

As the wireless medium is open to any device in the transmission range, anonymity concerns and solutions expand to many layers in the protocol stack. Underlying these techniques, mobility plays an important role on how effective they are when wireless eavesdropping techniques, encryption methods, user traffic patterns, and motion patterns can all be different. In addition, the security model of each design can be different, and it is needed to formally measure the effectiveness of a design. The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [8]:

• **Physical layer:** responsible for frequency selection, carrier frequency generation, signal deflection, data encryption and modulation. This is the layer that suffers the most damage from radio jamming attacks.

• **Data link layer:** responsible for the multiplexing of data streams, data frame detection, medium access control (MAC), data encryption and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections. This layer and more specific MAC are heavily damaged by link-layer jamming. In link-layer jamming [9], sophisticated jammers can take advantage of the data link layer to achieve energy efficient jamming. Compared to radio jamming, link-layer jamming offers better energy efficiency.

• **Network layer:** responsible for specifying the assignment of addresses and how packets are forwarded.

• **Transport layer:** responsible for the reliable transport of packets and data encryption.

• **Application layer:** responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.

IV. MULTIPATH ROUTING DESCRIPTION

Mobile ad hoc networks are characterized by a dynamic topology, limited channel bandwidth and limited power at the nodes. Because of these characteristics, paths connecting source nodes with destinations may be very unstable and go down at any time, making communication over ad hoc networks difficult. On the other hand, since all nodes in an ad hoc network can be connected dynamically in an arbitrary manner, it is usually possible to establish more than one path between a source and a destination. When this property of ad hoc networks is used in the routing process, we speak of multipath routing. The process of discovering multiple routes among the distinct source and single destination at the time of single route discovery corresponds to multi-path routing [4]

In most cases [10], the ability of creating multiple routes from a source to a destination is used to provide a backup route. When the primary route fails to deliver the packets in some way, the backup is used. This provides a better fault tolerance in the sense of faster and efficient recovery from route failures.

Multiple paths can also provide load balancing and route failure protection by distributing traffic among a set of disjoint paths.

Paths can be disjoint in two ways: (a) link-disjoint and (b) node-disjoint. Node-disjoint paths do not have any nodes in common, except the source and destination, hence the do not have any links in common. Link-disjoint paths, in contrast, do not have any links in common. They may, however, have one or more common nodes clearly shown figures 1 & figure 2.

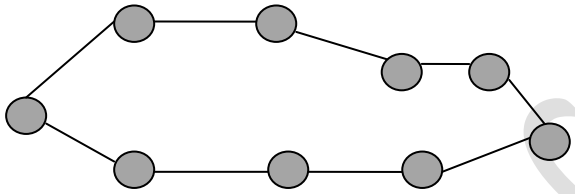

Fig. 1 Node-disjoint paths from source S to destination D

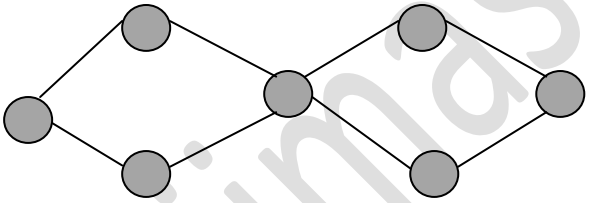

Fig. 2 Link-disjoint paths from source S to destination D

Multipath routing allows the establishment of multiple paths between a single source and single destination node. Multipath routing is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing.

V. PREVIOUS WORK AGAINST JAMMING ATTACK

In the literature, there are several proposals to detect such malicious hosts inside the network. In those methods, a baseline profile, which is defined as per static training data, is usually used to verify the identity and the topology of the network, thus preventing any malicious host from joining the network.Let's look out various researches already done by various researchers.

In this research [11] author focus on identified the vulnerabilities of routing protocols that fail to provide reliable routing and thus cause drastic degradation of data delivery performance under jamming. Pulse jamming that allows intermittent success in data delivery to jammed nodes is more efficient than constant jamming. Effective and efficient jamming attack can be executed through a careful selection of jamming rate based on routing protocol operations.

Drawbacks

- Only the mathematical calculation is identified the jammed region in network. It means only the jammed reason is identified. If the whole network is jammed, then this condition is not included.
- The PDR is 100% then how to prove network is jammed.
- Jamming attacker scenario considered with different bits capacity.
- How the RREQ and RREP is forwarded in jammed region not clear.
- The AOMDV routing performance is not evaluated in term of packets in network.

This paper [12], present a new type of denial of service attack (DJN) to wireless network. DJN is a combination of large number of tiny low power jammers that is motivated by the advancement in radio technology. DJN can cause a phase transition in target network performance even when the total jamming power is constant and investigated the impact of DJN topology on the jamming effectiveness.

This paper [13] present surviving attack in challenged network. That means a disaster event inside the telecommunication infrastructures can be easily damaged or overloaded, this time movement action network provide the communication services in ad hoc manner. This paper is proposed a general security framework for monitoring and reacting to disruptive attacks. Paper are presented modular framework for attack survivability in intermittent connected MANET composed of detection, diagnosis, mitigation and adaptation components.

P.Yi, Z.Dai, Y. Zhong and S.Zhang in [14] considered a route request (RREQ) flooding attack in MANETs. They proposed a RREQ flooding prevention mechanism based on neighbour's supervision that maintains a priority queue of the incoming RREQs. This mechanism reduces the priority of RREQs generated by a specific node if a higher rate of incoming queries from that particular node is observed. Here, the neighbours maintain a priority queue of incoming RREQs and reduce the probability of processing RREQs from a node if a high number of incoming RREQs are received from this node. If the number of RREQs received from a node exceeds a threshold the node neighbours cut off the path.

Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato in [15],proposed a new dynamic anomaly detection system for MANETs has been proposed. For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. To differentiate an attack state from the normal state, we have defined multidimensional features based on the characteristics of these attacks and utilized the projection distance using PCA based on statistical theory.

H. Deng, W. Li, and D. Agrawal [16] proposed an approach that requires the intermediate nodes to send a route reply (RREP) packet with the next hop information. When a source node receives the RREP packet from an intermediate node, it sends a "Further Request" packet to the next hop to verify that it has a route to the intermediate node and a route to the destination. As a response to this request, the intermediate node will send another RREP packet. When the next hop receives a "Further Request" packet, it sends a "Further Reply" packet that includes the verified result to the source node. Based on the information in the "Further Reply" packet, the source node judges the validity of the route.

S. Lee, B. Han, and M. Shin in [17] requires the intermediate node to send the route confirmation request (CREQ) to the next hop node toward the destination, and then, the next hop node receives the CREQ and looks into its cache for a route to the destination. If it has such a route to the destination, then it sends a route confirmation reply (CREP) message to the source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP.

In these methods [16, 17] the routing protocol has to be modified. These modifications may increase the routing overheads, which results in the performance degradation of the bandwidth-limited MANETs.

VI. PROPOSED SCHEME TO RECOGNIZED JAMMING ATTACK

When the source node sends the next block of data, the IDS nodes that are neighbors to the suspected nodes turn into licentious form and eavesdrop whether the data packets are forwarded or inundated by the suspected attacker nodes. If any of the suspected nodes is found to be inundated data packets intentionally, it will be moved to the malicious node list. Then a block of message is sent to all the nearby nodes by the IDS nodes which monitored them. Any IDS node that identified the jamming attacker will broadcast the block message to its neighbors and hence the malicious node is isolated from the network. The block message is forwarded only by the IDS nodes to the network. Any normal node that receives the block message will learn the malicious node information and then drop the message without forwarding. Once the malicious node is located and isolated, all nodes remove any routing information involving the attacker node from their route cache and no future RREP involving the malicious node is considered. The following steps by IDS are applied to detect and prevent from Jamming attacker.

1. In normal routing the sender ahs sends the RREQ (Route Request) to neighbor according to routing protocol AOMDV.
2. The sender and intermediate nodes are receives RREP from the nodes or destination if they receives RREQ packets.
3. The normal more than two paths are established through AOMDV and the data is forwarded to shortest path.
4. The jamming attacker continuously inundated the jamming packets or control message to all neighbors.
5. The attackers are not send heavy inundated packets but in every flooding the quantity of packets are increases.
6. It implies that the attacker gradually effect the network performance.
7. The proposed security IDS scheme is identified the attacker by their ‘Control Message’ that is only transmitted by attacker in network.
8. The IDS capture the particular information of node like Node Identification and Control messages. In that case only attacker is responsible for that kind of routing misbehavior.
9. The IDS block the misbehavior activities of attacker and provides the alternative path for communication of nodes.
10. The proposed scheme is provides the attacker free network and provides better routing performance through AOMDV protocol.

An ideal intrusion detection model in MANET should first have a reliable, distributed, low-overhead, message collecting, and exchanging mechanism. The mechanism should also adapt to changes in the network topology and tolerate message loss. Second, the model should be affordable for low computation in packets identification in term of node energy. . Third, the Secure IDS perform provides the protections since the routing topology may change very quickly and the attack damage may also propagate relatively quickly. Finally the route information is maintained for secure communication.

VII. SIMULATOR TOOL USED

The description about simulation environment is as follows:

Network simulator 2 (NS2) version NS-2.31 is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [18]. It is a discrete event simulator targeted at networking research. By simulation we analyze the performance of routing protocols for Mobile Ad hoc networks using scenario based experiments. It provides substantial support for simulation of all layer protocols, routing, multipath protocol, jammer attacker and security scheme. The standard ns-2 distribution runs on Linux. However, a package for running ns-2 on Cygwin (Linux Emulation for Windows) is available. In this mode, ns-2 runs in the Windows environment on top of Cygwin

The following network parameters are considered for simulation is radio range of mobile nodes is 500meters in this range the nodes are here to each other in network. Nodes are freely a move in the simulation area is of 800m*600m. Two ray ground propagation a model is used to propagation for signals. The number of nodes are considered total 50 in network and the number of sender and receiver are consider 12 nodes and rest of the nodes are normal nodes excluding the jammer attackers and protector nodes. The traffic generated at application layer through CBR with transport layer UDP protocol and FTP with transport layer TCP protocol and the packet size is of 512 bytes.

VIII. SIMULATION RESULTS

The simulation results on the basis of given parameters are evaluated in presence of AOMDV, Jamming attack and Proposed security scheme.

A. Jammer contamination Analysis

The jammer contamination analysis of AOMDV, Jamming and secure IDS scheme is signifies in this graph. Here the drop percentage is measure about 45%, due to effect of jamming packets in network. The drop percentage or contamination in routing is identified only in jamming attacker module. In case of secure IDS the drop percentage due to attacker is zero in network. The proposed scheme is effective and blocks the misbehavior activities of attacker and provides secure communication in presence of jamming attacker.

International Journal of Multidisciplinary Approach and Studies
ISSN NO:: 2348 – 537X

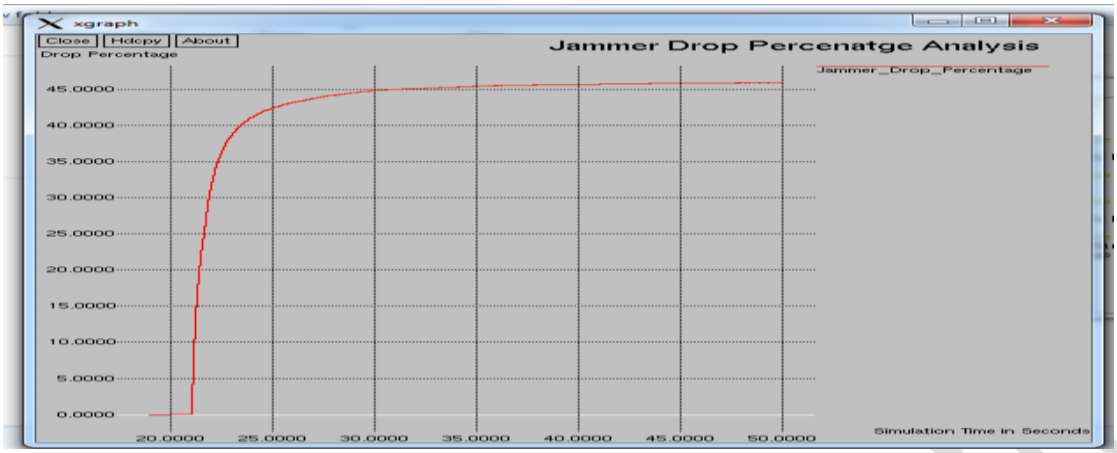

Fig. 1 Jammer Drop Analysis

B. Jammer node Identification

The jammer attacker nodes packets flooding are stated in table 1. Here we identified that the nodes 16, 17 and 18 are flooded huge number of packets in network to consume network bandwidth in network but node number 48 is the receiver node that only receives some packets by that their entry is exist in contaminated nodes. The IDS has blocked the misbehavior of attacker and provides zero flooding through these nodes in MANET.

Table 1 Attacker Node Analysis

Contaminated Nodes	*Total Infected Packets*
16	231412
17	231460
18	226368
48	570

IX. CONCLUSION & FUTURE ENHANCEMENT:

The decentralized communication of mobile nodes in MANET not secure because the attackers are easily accomplishes routing misbehavior. For that concern the security issues have become more important. Traditional defense lines are not sufficient for such networks, since they present different characteristics and properties that require new approaches. In this research we proposed IDS security scheme against jamming attack in decentralized MANET. The IDS security scheme id identified the loss of percentage because of attacker and block the attacker misbehavior by the attacker is tolly disabled in network and produces zero loss percentage because of attacker in MANET. The survivability concepts and its correspondence with preventive, reactive and lenience defense lines. Survivable MANETs will be able to fulfill their goals (even in the presence of attacks or intrusions) Due to the fact that the MANET environment dynamically keeps evolving, envisioning a robust proposed detection method becomes imperative to prevent the malicious attacks against it. The simulation results are illustrating the performance of security scheme in presence of jamming attacker in decentralized MANET.

In future the details and description of proposed security scheme is mention more briefly and also with respect to that presents the security scheme in detail and also evaluated the routing performance metrics like routing load, throughput and delay in network. The flooding of packets enhanced the routing load in network and prevention security scheme provides the normal performance in presence of jammer attacker.

REFERENCES:

i F. Adelstein, S. K. S. Gupta, and G. G. Richard III. Fundamentals of Mobile and Pervasive Computing. Mc Graw-Hill, 2005.

ii R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable Network Systems: An Emerging Discipline (cmu/sei-97-tr-013). Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1997.

iii B. Wu, J. Chen, J. Wu, and M. Cardei. Wireless/Mobile Network Security, chapter A survey on attacks and countermeasures in Mobile Ad hoc Networks. Springer, 2006.

iv S. R. Biradar, Koushik Majumder, Subir Kumar Sarkar, Puttamadappa, "Performance Evaluation and Comparison of AODV and AOMDV" International Journal on Computer Science and Engineering Vol. 02, No. 02, pp. 373-377, 2010.

v Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, " A Survey on Jamming Attacks and Countermeasures in WSNs", IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, pp. 43-56, Fourth Quarter 2009.

vi Radio Jamming- wikipedia. Available on link http://en.wikipedia.org/wiki/Radiojamming

vii Radio Jamming Info. http://www.radiojamming.info/

viii I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A Survey on Sensor Networks”, IEEE Commun. Mag., pp. 102-114, August 2002.

ix Y. Law, P. Hartel, J. den Hartog, and P. Havinga, “Link-layer jamming attacks on S-MAC” in IEEE 2nd European Workshop on Wireless Sensor Networks (EWSN), pp. 217-225, 2005.

x S. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad hoc Networks." Proceedings of IEEE WCNC 2000, Chicago, pages 1311-1316, September 2000.

xi Jae-Joon Lee And Jaesung Lim, "Effective And Efficient Jamming Based On Routing In Wireless Ad Hoc Networks", IEEE Communications Letters, Vol. 16, Pp. 1903-1906, No. 11, November 2012.

xii Hong Huang “On a New Type of Denial of Service Attack in Wireless Network: The Distributed Jammer Network” IEEE Transaction on Wireless Communication, vol. 10. No. 7, pp.2316-2324July 2011.

xiii Jordi Cucurull, Mikael Asplund, Simin Nadjm-Tehrani, Member, IEEE, 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,

xiv P.Yi, Z.Dai, Y. Zhong and S.Zhang, “Resisting Flooding Attack in Ad Hoc Networks”, Proceeding of IEEE International Conference on Information Technology Coding & Computing (ITCC), pp. 657-662, April 2005.

xv Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, " A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 58, No. 5, pp. 2471-2481, June 2009.
xvi H. Deng, W. Li, and D. Agrawal, "Routing security in ad hoc networks," IEEE Communication Magzine, Vol. 40, No. 10, pp. 70–75, October 2002.
xvii S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in Proceeding 31st ICPP Workshops, pp. 73–78. August 2002.
xviiiNS--2utorial for studying and practice available on the link: http://www.isi.edu/nsnam/ns/tutorial/nsindex.html