International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure Detection and Prevention Scheme for Jamming Attack in MANET

Ashwini Magardey[1], Dr. Tripti Arjariya[2]

[1]M. Tech. Scholar in Department of CSE, Bhabha Engineering Research Institute, Bhopal, India.

[2]Department of CSE, Bhabha Engineering Research Institute, Bhopal, India

Abstract: ***In MANET, secure routing is the major issue and it is difficult to identify malicious hosts as the topology of the network dynamically changes. In this paper we proposed the security scheme against jamming attack with AOMDV protocol. The proposed IDS scheme is identified the jammer attacker through the flooding of number of misbehavior control packets. These control packets are only consumes the network bandwidth and after some time it blocks the whole channel. Because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious routing behavior performed by a compromised node in network but the proposed scheme is identified it without any overhead in routing performance. The proposed IDS (Intrusion Detection System) security scheme is identified the attacker by their routing entry present on other nodes routing record. 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 performance metrics like throughput, routing load is evaluated and observe the secure proposed security scheme is immobilized the routing misbehavior of jamming attacker and provides secure AOMDV routing performance as equal to normal AOMDV performance.***

Keywords: Routing, Jamming attack, IDS, AOMDV, MANET

1. Introduction

A mobile ad-hoc network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust. Two non-adjacent devices can communicate only if other devices between them are in MANET and are willing to forward packets for them. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. Because of lack of centralized administration, all the network activities like discovering of topology and message delivering are executed by nodes themselves. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. Mobile ad-hoc networks are inclined to a large number of security threats [2].

The basic reality that MANET lack permanent infrastructure and use wireless link for interaction makes them very predisposed to an adversary's spiteful attacks. Attackers are severe security threats in ad-hoc networks which can be employed with no trouble by exploiting susceptibility of on-demand routing protocols such as AODV. The intrusion Detection System (IDS) is not only detects the attack malicious but also prevents attacks imposed by both single and multiple nodes and the Detection and healing routing misbehaviour under MANET [3]. we try to reach up to the specific solution maximizes network performance by the help of minimizing production of control (routing) packets as well as successfully opposing attacks against mobile ad-hoc networks [1]. One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. This last point is where the main problem for MANET security resides the MANET can be reached very easily by users, but also by malicious attackers.

The routing protocols in MANET are basically classified in three categories [4] like proactive, reactive and hybrid. The Multipath protocol like AOMDV [5] is established more than one path for data sending and receiving in MANET.

The open wireless medium in MANETs renders secure neighbor discovery particularly vulnerable to the jamming attack, in which the adversary intentionally transmits noise like signals to prevent neighboring nodes from exchanging messages and thus discovering each other at physical layer but at time of routing the huge packets are sending by attacker. In jamming the communicating parties flooded the unauthorized packets (unknown to the adversary) to spread the signals such that the transmissions are unpredictable and thus resilient to jamming [6]. Failure in data delivery ends up compromising the reliability of the network and thus war operation in question. In the battlefield where mobile ad hoc networking technologies are used, electronic attacks like jamming by the enemy is highly probable to prevent tactical communication. Jamming attacks in radio networks is the deliberate transmission of radio signals by adversaries to disrupt communication through interference and cause data delivery failures by attacker in MANET.

In this paper we proposed the IDS security scheme against jamming attack with AOMDV routing protocol. The attacker is identified from their unnecessary routing message flooding and IDS has blocked their participation in routing and provides secure communication.

2. Literature Survey

The let's look out various researches already done by various researchers. In this research [6] 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.

In this research [7] author focus on improving the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and black hole attacks. The performance analysis carried out shows improvement in packet delivery ratio in presence of black hole attack, with marginal rise in average end-to-end delay and normalized routing overhead. The proposed mechanism for flooding attack works even when the identity of the malicious nodes is unknown and does not use any additional network bandwidth. It is simple to implement and maintains or improves network throughput when there are no malicious nodes but the network is congested with excess traffic.

In this paper [8] we proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. We developed a probability model utilizing stochastic Petri nets techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. We demonstrated the feasibility of dynamic hierarchical trust management and application-level trust optimization design concepts with trust based geographic routing and trust-based IDS applications, by identifying the best way to form trust as well as use trust out of individual social and QoS trust properties at runtime to optimize application performance. Here trust-based IDS algorithm outperforms traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives.

The authors [9], discuss the different types of security attacks that can be launched easily in MANETs and related solutions needed for ensuring network security. This paper implements the secure ad hoc on-demand distance vector routing protocol (SAODV) and compares the performance of protocol with existing AODV protocol in the presence of black hole attack. Since public key cryptography is used in this scheme, it takes significant amount of time to compute digital signature at each node. Also, this leads to high overhead and processing power requirements.

In this paper author proposed FACES (Friend-Based Ad-hoc routing using Challenges to Establish Security) [10], that provides a list of trusted nodes to the source node by sending challenges and sharing friend lists. Based on the extent of successful data transmission and the friendship with other nodes in a network, the nodes in the friend lists are rated. The trust level of each node varies from -1 to 4. The nodes in the network are placed in one of the three lists, i.e. question Mark list, friend list and unauthenticated list. The periodic flooding of challenge packet and sharing of friend lists increases the control overhead.

In this paper [11] author proposed per-IP traffic behavioral analysis, in this they present a real time DDoS attack detection and prevention system which can be deployed at the leaf router to monitor and detect DDoS attacks. The advantages of this system lie in its statelessness and low computation overhead, which makes the system itself immune to flooding attacks. Based on the synchronization of TCP and UDP protocol behavior, this system periodically samples every single IP user's sending and receiving traffic and judges whether its traffic behavior meets the synchronization or not. A new nonparametric CUSUM algorithm is applied to detect SYN flooding attacks. Moreover, this system can recognize attackers, victims and normal users, and filter or forward IP packets by means of a quick identification technique. Moreover, this system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology.

In this [12] research, rejection of Service attack is applied in the network, evidences are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to find out the accuracy of detection engine by using support vector machine. Universal Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes similar to routing, and deciding the cluster head for scalable ad-hoc networks. Aspect takes out for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols..

In this approach [13] a message security approach in MANETs that uses a trust based multipath AOMDV routing combined with soft encryption, yielding our so-called T-AOMDV method. Replication results using ns2 exhibit that our scheme is much more secured than traditional multipath routing algorithms and a recently proposed message security scheme for MANETs. The performance criteria used are route selection time and trust compromise. This requirement poses a security challenge when malevolent nodes are present in the network. Indeed, the existence of such nodes may not simply disrupt the normal network operations, but cause serious message security issue concerns, from data availability, privacy, and/or integrity viewpoints.

In this paper [14], the current security issues in MANET are investigated. Universally, we have examined different routing attacks, like flooding, black hole, link spoofing, wormhole, and colluding miserly attacks, as well as existing solutions to protect MANET protocols. A MANET is a promising network technology which is based on a self organized and rapidly deployed network. Due to its excellent features, MANET attracts different real world application areas where the networks topology changes very rapidly. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks issues. In this paper

author discussed present routing attacks and countermeasures against MANET protocols.

3. Proposed Security Scheme against Jamming Attack

The proposed research is divided in to three modules like normal AOMDV routing, Jamming Attack and proposed IDS security scheme. The proposed steps to identified attacker is mentioned step by step in algorithmic foam. The IDS node identified the control packets load on the network. The IDS node is recognizes the port number of attacker to block

Max Load Limit = (total control Pks sends by S_n / 2) // recognize from normal AOMDV performance
If ((load > = max_limit) && (new table entry!= normal Table entry))
{
Capture control packets load on network of I_n nodes // Intermediate Nodes
Create normal Table of I_n nodes;
Create abnormal Table of I_n nodes;
Insert value into abnormal_table;
Find_attack_info();
Find_attacker_information(node_number, pkt_type, Load)
Capture infection type;
Infect percentage;
Attacker Port_number; // port number =1 (enable)
Attacker identified through IDS;
{
If (Upcoming Table Entry == abnormal table entry)
{
IDS Capture attacker node information from table entry;
Block the infected node; // by block the communication through Port number disable to from 1 to 0
Broadcast attacker node Identification in network;
}
Else
{
Packets enter in table and attacker not found;
}
}
Else
{
Control Packets delivery is normal and Attack not identified in network;
}
}

The attacker is MANETs introduce assorted functions, operations and services influenced by the context and malicious activities. In a critical situation, where parts of a system are compromised by attacks or intrusions, proposed IDS priority is given to maintain correct functionality of essential services. Essential services demand capacities and guaranties to assure their correct data delivery in the presence of jamming attack failures. Such capacities and guaranties are identified through strong security scheme and they can diverge significantly depending on the system characteristics, its scope, and the consequence of the service interruption. Survivable MANET in presence of IDS must maintain a connected network even in adverse situations, since that service allows efficient routing and end to end communication. The proposed IDS security finally manages them in order to optimize the use of their resources, minimizing latency and maintaining the quality of service of network.

4. Simulator Outline

dd Network Simulator -2 (NS-2) [15] is a network simulator tool. It is developed at UC Berkeley as a part of the VINT project. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS-2 simulator is an open source software and are easily available, compatible with Linux, Solaris, Windows and Mac OS X . The network simulator NS is a discrete event network simulator developed at UC Berkeley that focuses on the simulation of IP networks on the packet level. The NS project (the project that drives the development of NS) is now part of the Virtual Inter Network Testbed (VINT) project, which develops tools for network simulation research. NS is basically an Object-oriented Tcl (Otcl) script interpreter with network simulation object libraries. NS has a simulation event scheduler, network component object libraries and network setup (plumbing) module libraries.

A. Simulation Parameters

According to below table 1.1 we simulate our network on the basis of these simulation parameters.

Table 1.1: Simulation Parameter

Number of nodes	50
Dimension of simulated area	800×600
Routing Protocol	AOMDV
Work on Attack	Jamming attack
Simulation time (seconds)	50
Traffic type	CBR, FTP
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	Random

5. Results Evaluation

The simulation results on the basis of given parameters are evaluated in presence of AOMDV, Jamming attack and Proposed security scheme. The proposed scheme is provides the freedom from jammed network.

A. UDP End Packet Received Analysis

The UDP protocol is the connection less protocol for end to end data delivery in dynamic ad hoc network. The attacker had with no trouble exaggerated the receiving of that protocol connection in network. The jammer attacker exaggerated the performance and consumes the available bandwidth. This graph has give you a performance analysis of Jammer attacker and Secure scheme against Jamming attack. The packets received in jamming scenario is only about 90 packets are received but the proposed security scheme is block the routing misbehavior of attacker and received 1600 packets in network.

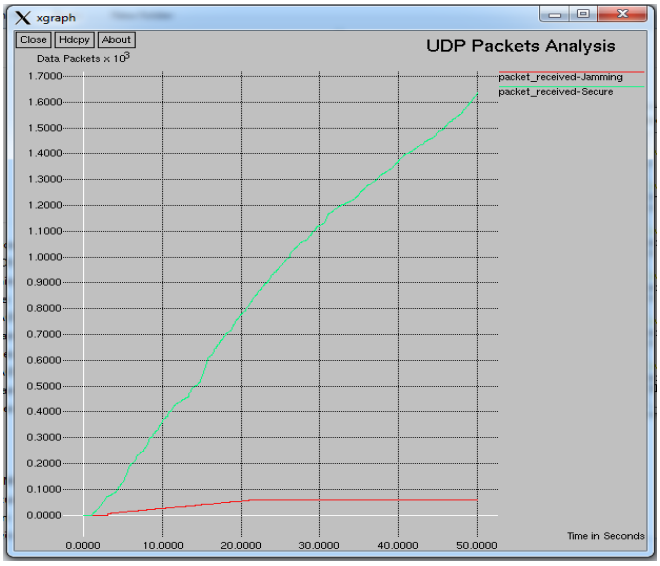

Figure 6.8: UDP Packets Received Analysis

B. PDR Analysis of Jamming Attack and Proposed Security Scheme

The attacker in MANET are easily exaggerated the routing misbehavior for the reason of independent establishment of network. The attacker aim is to drop the data packets or to hold the resources for that the communication is affected. The attacker drop of packets is humiliates the percentage ratio of data receiving. The packets percentage ratio or Packet Delivery Ratio (PDR) performance of Jamming attacker and Security scheme is specified in this graph. The PDR performance of attacker is only evaluated up to time 30 second in a simulation of 100 seconds. The attacker is obstructing the processing capability of nodes and bandwidth capacity, because of that the whole network is jam and PDR performance is not assessed. The Rest of the time only the attacker is flooding bogus connection establishment packets due to that up to end of simulation no PDR is value is count. The PDR performance of proposed security scheme is completely block the misbehavior of attacker and provides 90% receiving ratio and it is about 98 percent in some different time, undoubtedly shown in figure.

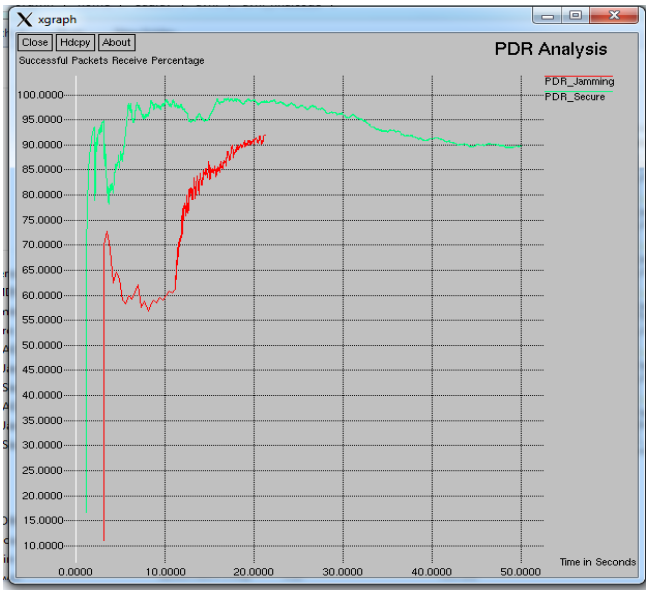

Figure 6.9: PDR Performance Analysis

C. Routing Load Analysis of Jamming Attack Security Scheme

The routing overhead performance is containing the measurement of number of data packets with respect to number of control packets in dynamic Ad hoc network. The routing flooding analysis of attacker and proposed security scheme is mentioned in given graph. In fact, in a jammaed network, where the high channel contention causes a degradation of the link reliability, the routing decision is mainly obsessed by the cost that models the quality of the link. The jammer attacker incessantly flooding the number of control packets, their calculation in given simulation time of 50 seconds is 420000 packets but the calculation is as certain change in scenario of security scheme. In security scheme the only little more than 1000 packets are flooding in network that shows the better performance and improves the link reliability by block the consumption bandwidth through attacker. In presence of security scheme the jammer attacker not produces an unwanted control packet.

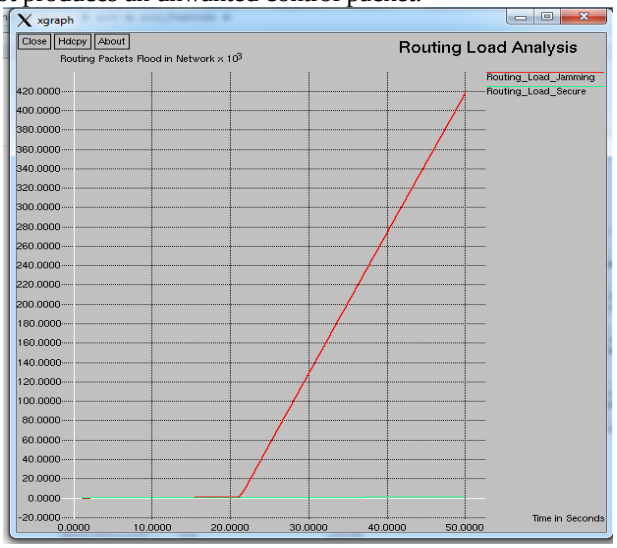

Figure 6.10: Routing Load Performance Analysis

D. Throughput Analysis of Jamming Attacker and Security Scheme

The packets forwarding capacity of jammer attacker is a strictly increase with a period of time, which causes the higher transmission of control packets forwarding in Ad hoc wireless network but the packets receiving capacity of intermediate nodes is limited for that reason the forwarding and receiving capacity is affected and after some time bandwidth is occupied by unwanted junk of jammer packets that causes the reason of degradation of network throughput. The throughput experimental performance is shown in this graph and observes the attacker is affected the throughput by block the link capacity. The throughput of attacker is evaluated only up to time 22 seconds after that the link is consumes by jammer generated packets but the proposed security scheme is steps forward the throughput up to maximum 1200 packets/seconds. The proposed security scheme is block the flooding of unwanted packets and provides normal network performance in existence of attacker.

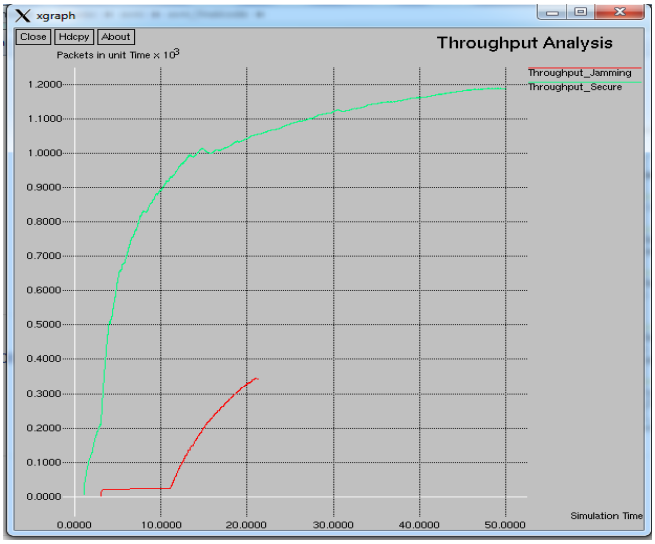

Figure 11: Throughput Performance Analysis

6. Conclusion and Future Work

The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic network. The MANET suffers from attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node or nodes in the network, which causes routing misbehavior in network. The AOMDV protocol are improves the routing capability and also ignores the path where the attacker is exists in network. The IDS security scheme id identified the loss of percentage because of attacker and block the attacker misbehavior by the attacker is totally disabled in network and produces zero loss percentage because of attacker in MANET. The simulation results are illustrating the performance of security scheme in presence of jamming attacker in MANET. The proposed security scheme is secure the network from attacker evaluated the routing performance metrics like routing load, throughput and delay in network. The routing performance of normal AOMDV protocol is equivalent to the proposed IDS security scheme, which represents the normal network performance in presence of attacker. The flooding of packets enhanced the routing load in network and prevention security scheme provides the normal performance in presence of jammer attacker.

In MANET the attacker is also consumes the communication resource like battery power due to that nodes are early going to sleep mode. In future we also work on resource consumption attack or vampire attack in MANET.

References

[1] S.Madhavi, “An Intrusion Detection System in Mobile Ad Hoc Networks”, International Journal Of Security And Its Applications Vol. 2, No.3, Pp. 1-16, July, 2008

[2] Sunilkumar S. Manvi, Lokesh B. Bhajantri, And Vittalkumar K. Vagga, “Routing Misbehavior Detection In Manets Using 2ACK”, Journal of Telecommunication and Information Technology (JTIT), pp. 105-111, 2010.

[3] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, pp. 2027-2043, Fourth Quarter 2013.

[4] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma "Review of Various Routing Protocols for MANET" International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[5] Marina, M.K., Das, S.R., "On-demand Multipath Distance Vector Routing in Ad Hoc Networks" IEEE Proceedings of the International Conference for Network Protocols (ICNP), 2001.

[6] Jae-Joon Lee And Jaesung Lim, "Effective and Efficient Jamming Based nn Routing in Wireless Ad Hoc Networks", IEEE Communications Letters, Vol. 16, Pp. 1903-1906, No. 11, November 2012.

[7] 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.

[8] 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

[9] Preeti Sachan, Pabitra Mohan Khilar, “Security Attacks and Solutions in MANET”, Proceedings of International Conference on Advances in Computer Engineering (ACEEE), Pp 172-176, 2011.

[10] 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.

[11] Yi Zhang, Qiangliu “A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Pp. 163 – 167, 2010.

[12] Husain. Shahnawaz, Gupta S.C., Chand Mukesh “Denial Of Service Attack in AODV & Friend Features Extraction to Design Detection”, IEEE International Conference On Computer & Communication Technology (ICCCT), pp. 292-297, 2011.

[13] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, “Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks”, Publication in the IEEE Globecom 2011.

[14] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, International Journal Of Computer Science And Security, Volume 2, 2008.

[15] Marc Greis's tutorial (now maintained by VINT group), available on http://www.isi.edu/nsnam/ns/tutorial/index.html.