International Journal of Latest Research In Engineering and Computing (IJLREC) ISSN:2347-6540
Volume 1, Issue 2 : Page No26-33, November-December 2013
www.ijlrec.com

A New Algorithm For Secure Routing Protocols For Moble Adhoc Networks

[1]Kailash Pareek, [2]Prof. K.P. Yadav
[1]Research Scholar, Singhania University, Rajasthan, India
[2]Professor, SIET, Ghaziabad, U.P., India

Abstract :- A mobile ad hoc network is a collection of wireless nodes that can be rapidly deployed as a multi-hop packet radio network without the aid of any existing network infrastructure or centralized administration. Therefore, the interconnections between nodes are capable of changing on continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Key Words: Cellular network, adhoc network, mobile network security.

Introduction

In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, thus opening new fields of applications in the domain of networking. One of the most important of these fields concerns Mobile Ad hoc Networks (MANETs) where the participating nodes do not rely on any existing network infrastructure. A mobile ad hoc network is a collection of wireless nodes that can be rapidly deployed as a multi-hop packet radio network without the aid of any existing network infrastructure or centralized administration. Therefore, the interconnections between nodes are capable of changing on continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Ad- hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

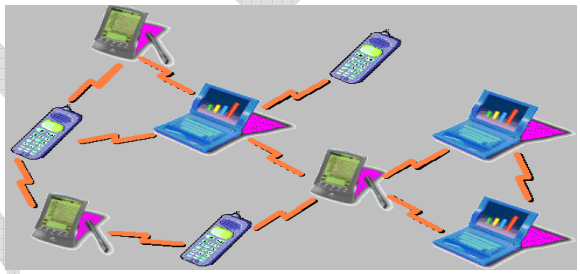


Figure 1 : An Overview of MANET

Cellular network technologies were developed to allow mobile phones to connect via base stations and communicate in a circuit switched environment. The area of mobile ad-hoc networking deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points. Wireless devices form a network as they become aware of each other's presence. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired network using radio wave technologies through wireless access points. Simultaneously, telephone networks were undergoing a similar transformation.

Meaning of Adhoc Networks

On wireless computer networks, **ad-hoc** mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate

in peer-to-peer fashion without involving central access points (including those built in to broadband wireless routers). An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wired LANs or to the Internet without installing a special-purpose gateway.
Mobile adhoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid of establish infrastructure. In mobile adhoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes in underlying protocol design and lack of centralized monitoring and management point. The main aim of this work is to provide secure data transmission between the source and destination. The simulation is carried out for different number of mobile nodes using network simulator with the help of 1000 mobile nodes. We have compared this model with the existing models such as DSR and AODV. This model has shown the better results in terms of packet delivery, packet drop, and delay. The proposed model has dropped 19% of the packets even if network has five malicious nodes.

Routing protocol

The paths are maintained as long as source needs. Here, we use sequence numbers to maintain the up-to-date information. The routing information has been updated using Route Request RREQ packet. If the source wishes to communicate with destination, for which it does not have a path, then it broadcast the RREQ packet to the network. After receiving, the intermediate node will broadcast a Route Reply(RRE) packet. If the RREQ packet has already processed, then it will be discard. The proposed model uses Zonal Routing Protocol(ZRP). Here, each node proactively maintains a set of possible routes within the region. Knowledge of each region is learned by the ZRP to improve the network performance efficiency. The DSDV is used to learn about nodes within the region. In order to find the routes for nodes, which are out-of-region and DSR is used.

EXISTING WORK of Algorithm in MANETs

The secure routing algorithms in wireless communication are addressed and have been suggested for increasing the security levels. However, these algorithms are unable to protect the network from attackers, who acquired the key information. *J. Li et al* proposed a common key encryption mechanism for MANETs using Dynamic Source Routing (DSR). Drawback of this model is that it dropped more packets even if the network had few malicious users. Adhoc On-Demand Distance Vector (AODV), which is used to provide secure and reliable data transmission over the MANETs. Several strategies are used to detect the non-cooperate nodes while forwarding the data packets to the destination. In, authors discussed a trusted approach to establish the communication between the mobile users. Here, the communication takes place based on the watch dog. The trusted values are represented from -1 to +1.

A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Smith *et al* examined the routing security of distance vector protocols in general and developed countermeasures for vulnerabilities by protecting both routing messages and routing updates. They propose sequence numbers and digital signatures for routing messages and updates as well as including predecessor information in routing updates.

Categories OF MANETs

There are three different categories of MANETs including:

1 InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.

2 Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

3 Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to Communicate with roadside equipments.

The Features of Ad hoc Networks

1. In MANET, each node act as both host and router. That is it is autonomous in behaviour.
2. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
3. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
4. Mobile and spontaneous behaviour which demands minimum human intervention to configure the network.

5. All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
6. High user density and large level of user mobility.
7. Nodal connectivity is intermittent.
8. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
9. The nodes can join or leave the network anytime, making the network topology dynamic in nature.
10. Mobile nodes are characterized with less memory, power and light weight features.

Goals of Networked Security

Secure networking environment some or all of the following services may be required: It ensures that the intended receivers can only access the transmitted data. This is generally provided by encryption. Any data transmitted between the nodes is encrypted using this key. This key must be provided to the nodes over a secure channel. Symmetric encryption generally requires less computational resources than public key encryption. Public Key Encryption, where all nodes participating generate a public\private key pair puck/ proven. The node makes its public key puck available to all nodes. If other nodes wish to send data to node n, they encrypt their data using puck, safe in the knowledge that it can only be decrypted by n's private key proven, which only node n knows. Ensures that the data has not been altered during transmission. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.
Both sender and receiver of data need to be sure of each other's identity. It intended network security services listed above are available to the intended parties when required. The availability is typically ensured by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocols. This is a vague metric and is provided in varying degrees by all security protocols. The use of multi hop wireless networks can help keeping the power consumption down due to lowering the link length. However, the need to make the routing protocols power aware and not waste too much power on control messages instead of actual information traffic is essential. Also, multi hop networks are dependent on the intermediate nodes being available even though that node may not be in transceiver mode. The use of multiple available routes might be a solution where some nodes can go down in power saving mode while others peek up now and then to sense the communications.When all the traffic starts to flow around between everybody seemingly uncontrolled the need forsecurity and authentication arises. This is what the rest of this thesis will focus on.

Research Proposal Model

This model presents a secure communication between the mobile nodes. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node via the cluster head. The authentication service uses a key management to retrieve the public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source. After execution of the key management module, a session key is invoked, this is used by both source and destination for further communication confidentially. In this way, all the important messages are transmitted to the destination.

SIMULATION

This model has considered an area of 1000mX1000m with a set of mobile nodes placed randomly and broadcast range is 150m. The simulation was carried out for different number of nodes using Network Simulator(NS2). The node mobility is simulated with a velocity of 0-20m/s. It sends 30000CBR packets approximately and the simulation parameters are shown in Table I. The performance metrics are packet-delivery ratio, throughput and control message packet.

Network Threats

Any network, wireless or wire-line, is subject to substantial security risks and issues. These include:

a) Threats to the physical security of a network
b) Unauthorized access
c) Privacy

Physical Security

Given the obvious reliance of wire-line networks on the wire, anyone gaining access to that wire can damage the network or compromise the integrity and security of information on it. Without the proper security measures in place,

even registered users of the network may be able to access information that would otherwise be restricted. Disgruntled current and ex-employees have been known to read, distribute, and even alter valuable company data files. Network traffic can be intercepted and decoded with commonly available software tools once one has physical access to the network cabling. In a wire-line network including cable systems, countless cases have been documented of wiretapping, hacking by authorized users and even people down the street hacking into their neighbor's computers.

Table 1: some Simulation parameters

Simulation time	2000s
Topology size	1000mX1000m
No. of nodes	1000
No.of clusters	10
No.of cluster heads	10
No. of malicious nodes	7
Node mobility	0 to 10m/s
Transmission range	250m
Routing protocol	ZRP
Frequency	2.4Ghz
Channel capacity	2Mbps
Traffic type	CBR
CBR packet size	512 bytes
Number of packets	30000
Simulator	NS2
Communication system	IEEE802.11g
Pause time	1s
Mobility model	Random way
Total packets	30000

Subscribers, regardless of whether or not they have wireless segments on their networks, need to have the appropriate security products for their environments, the proper security levels set for their users, and an on-going process to audit the effectiveness of security policies and procedures. Physical access to network wires needs to be protected.
Unfortunately, the vast amount of wire inherent in most networks provides many points for unauthorized access.

Unauthorized Access

Another area of concern for security-conscious subscribers is the growing use of the Internet. Often, if users from inside can get out to the Internet, then users from outside can get into a network if proper precautions haven't been taken. And this applies not only to the Internet, but also to any remote network access capabilities that might be installed. Remote access products that allow traveling sales and marketing people to dial in for their email, remote offices connected via dial-up lines, intranets, and "extranets" that connect vendors and customers to a network can all leave the network vulnerable to hackers, viruses, and other intruders. Firewall products offering packet filtering, proxy servers, and user-to-session filtering add additional protection.

Privacy

Perhaps the most difficult threat to detect is someone just looking at (and likely copying) raw data on the network. Wire-line networks are particularly vulnerable to eavesdropping. Most Ethernet adapters on the market today offer a "promiscuous mode" that, with off-the-shelf software, enables them to capture every packet on the network. Most network administrators have some kind of "packet sniffer" and/or network traffic analyzer for trouble-shooting the network. Inexpensive and readily available hardware and software let anyone with physical access to the network to read, capture, and display any type of packet data on the net. While data encryption is the only line of defense against this kind of threat unfortunately, no wireline network service provider incorporates this technology as even an option that subscribers could use with their product.

Problem Statement

Mobile ad hoc networking (MANET) bring great challenges in security due to its high dynamics, link vulnerability and complete decentralization. With routing being a critical aspect for MANETs, existing routing protocols however are not sufficient for security requirements. In this paper, we present a route discovery algorithm that mitigates the detrimental effects of malicious behavior, as to provide correct connectivity information. Our algorithm guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying

node. Furthermore, the algorithm responsiveness is safeguarded under different types of attacks that exploit the routing algorithm itself. The sole requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. Specifically, no assumption is made regarding the intermediate nodes, which may exhibit arbitrary and malicious behavior. The scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner.
The end-nodes are enabling QoS such as end-to-end delay, packet-loss, throughput and secure data transmission. The potential deployment of MANETs exists in many scenarios, for example in situations where the infrastructure is not feasible such as disaster relief and cyclone, etc.

OBJECTIVE OF THE STUDY

Network performance depends to a great extent on giving participating nodes an incentive for cooperation .Mobile ad hoc networks rely on cooperation to perform essential network mechanisms such as routing. The level of trust among nodes is the most frequently used parameter for promoting cooperation in distributed systems. There are different models for representing trust, each of which is suited to a particular context and leads to different procedures for computing and propagating trust. The goal of this study is to analyze the most representative approaches for surveying and analyzing of mobile ad hoc networks. It aims to obtain a qualitative comparison of the modeling approaches, according to the three basic components of a trust model: information gathering, information scoring and ranking, and action execution.

Research Methodology

Practically, in a MANET, most devices have very limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some of the mobile devices would not like to forward the packets for the benefit of others and they drop packets not destined to them. On the other hand, they still make use of other nodes to forward packets that they originate. These misbehaved nodes are very difficult to identify because we cannot tell that whether the packets are dropped intentionally by the misbehaved nodes or dropped due to the node having moved out of transmission range or other link error. Packet drop significantly decreases the network performance. This research study examine " **A NEW ALGORITHM FOR SECURE ROUTING PROTOCOLS FOR MANETs".** Formulation of networking probations is the foundation of all scientific research work as it gives direction to inquiry and helps the researcher to draw specific conclusion. The research topic be defined as tentative solution to the problem which can be put to determine its validity.

Review of Literature

All the dynamical feedback mechanisms investigated in chapter 3 rely on inherent redundancies – multiple routes available to a single destination. As long as there are enough good nodes and alternative routes, packets can go around those misbehaved nodes and arrive at a destination. Thus increasing the number of available routes to the same destination is very important. The route cache is used to store routes in the standard DSR. When a node gets a new route, either by initiating a new route discovery or by overhearing a packet that contains route information, it adds the route into the route cache. When the node wants to send a packet to a destination node, it searches a shortest route to the destination in the route cache. If no route is found, the node will send out a Route Request to find new routes. With standard DSR, a node selects a shortest route to the destination from the route. Network topologies and memberships are constantly changing.

1. **Hierarchical routing protocols :**
   With this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels.

2. **Back pressure routing :**
   It is an algorithm for dynamically routing traffic over a multi-hop network by using congestion gradients. The algorithm can be applied to wireless communication networks, including sensor networks, mobile ad-hoc networks, and heterogeneous networks with wireless and wire line components. Backpressure principles can also be applied to other areas, such as to the study of product assembly systems and processing networks.
3. **Power-aware routing protocol :**
   Energy required to transmit a signal is approximately proportional to d^{α}, where d is the distance and $\alpha \geq 2$ is the factor or path loss exponent, which depends on the transmission medium. When $\alpha = 2$ (which is the optimal case), transmitting a signal half the distance requires one fourth of the energy and if there is a node in the middle willing to spend another fourth of its energy for the second half, data would be transmitted for half of the energy than through a direct transmission – a fact that follows directly from the inverse law of physics.
4. **Multicast routing :**
   A number of emerging network applications require the delivery of packets from One or more senders to a group of receivers. These applications include bulk data Transfer (for example, the transfer of a software upgrade from

the software developer To users needing the upgrade), streaming continuous media (for example, the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants), shared data applications (for example, a whiteboard or teleconferencing application that is shared among many distributed participants), data feeds (for example, stock quotes), Web cache updating, and interactive gaming (for example, distributed interactive virtual environments or multiplayer games such as Quake). For each of these applications, an extremely useful abstraction is the notion of a multicast: the sending of a packet from one sender to multiple receivers with a single send operation.

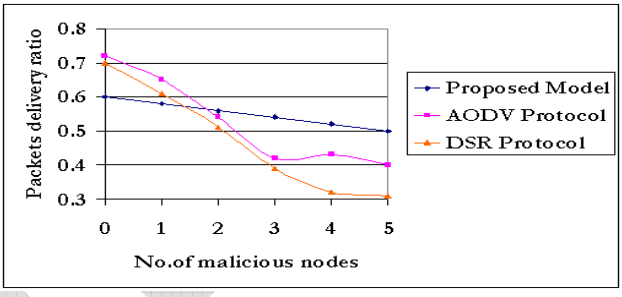
5. On demand data delivery routing :

On-demand routing protocols were designed to reduce the overheads in Table-Driven protocols by maintaining information for active routes only. When a node requires a Route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. Route discovery usually occurs by flooding a route request packets through the network. When a node with a route to the destination (or the destination itself) is reached a route reply is sent back to the source node using link reversal if the route request has traveled through bidirectional links or by piggy-backing the route in a route reply packet via flooding.

SIMULATION RESULTS

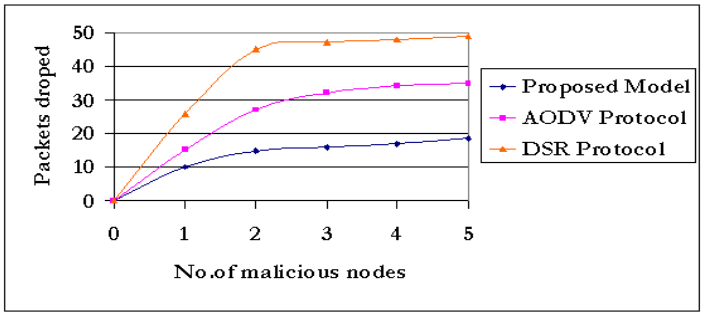
We consider 250 mobile nodes (5 malicious nodes) and 3 cluster heads, number of data packets sends between 5-20 packets/s, and each node moves with 8 m/s. We have executed our model with different arrival of rates of packets for 20times. The simulation results are shown in Figure 2. From the results, we conclude that AODV protocol is delivered around 72% of the packets, while proposed model delivers 60%. For 5 malicious nodes, the proposed model delivers 51% of the packets due to packet loss caused, during the detection phase, i.e., after a malicious node has launched attacker yet before it is finally isolated, whereas AODV and DSR protocols have transmitted with 40% and 35% of the packets respectively.

Fig.1 : No. of malicious nodes versus packets deliver ratio



The next Fig. shows the number of data packets dropped by the malicious nodes, as total number of data packets is transmitted by the source. Here, we have considered 125 nodes(5 malicious nodes), 2 cluster heads, and number of packets sends between 0-80 packets/s and each node moves constantly with 2 m/s. In DSR model, 47% of the packets are caused by the malicious nodes, while AODV protocol has caused with 39% and the proposed model with 19% of the packets.

Fig.2 : Number of malicious nodes against packet dropped.



14. Trust Based Security Solutions

Research in Mobile Ad Hoc and Sensor Network security in general is the Trust Based Security Solutions. In Sun et al. have identified the role of Trust in MANETs. When a network entity establishes trust in other network entities, it can predict the future behaviors of others and diagnose their security properties. Trust helps in Assistance indecision making to improve security and robustness, Adaptation to risk leading to flexible security solutions, Misbehavior detection and Quantitative assessment of system-level security properties.

Conclusion and Future Scope

There are various MANETprotocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes. It allows the attackers to influence the victim's selection of routes or enable the denial- of service attacks. In this model, we have discussed the security issues for MANETs. It focuses on the security architecture. Since, every attack has own characteristics. One of the limitations of this model is that it works based on the assumption of malicious nodes, which do not work as a group. It may be happened in a real situation.

In our research, we present a variety of attacks related to different layers and find that network layer is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. The second question is ‘what are the countermeasures? How the security of the entire system is ensured?’ We focus on the potential countermeasures either currently used in wired or wireless networking or newly designed specifically for MANET in our research. We can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. The final research question is ‘what are the potential dangers that may be crucial in future?’ Everyday, the attackers are trying to find out the new vulnerability in MANET. But it is sure that the multi-layer or combined attacks will be vital for secure communication in MANET.

References

1. B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour,“A Survey Of Routing Attacks In Mobile Ad Hoc Networks,”IEEEWireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.
2. B. Williams and T. Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks," Proc. MobiHoc 2002, pp. 194-195.
3. C. Barrett et al., "Characterizing the Interaction Between Routing and MAC Protocols in Ad-hoc Networks," Proc. MobiHoc 2002 , pp. 92-103
4. C. Elliott and B. Heile, "Self-Organizing, Self-Healing Wireless Networks," Proc. 2000 IEEE Int'l Conf. on Personal Wireless Comm., pp. 355-362.
5. D. Wang, M. Hu, H. Zhi, “A Survey of Secure Routing in Ad HocNetworks,”IEEE Ninth International Conference on Web-AgeInformation Management, 2008, (WAIM '08), pp.482-486, July 2008.
6. D. Cavin et al., "On the accuracy of MANET simulators," Proc. ACM Workshop on Princ. Mobile Computing (POMC'02), Oct. 2002, pp. 38-43.
7. F. Baker, "An outsider's view of MANET," Internet Engineering Task Force document (text file), 17 March 2002.
8. Joo B. D. Cabrera, Raman K. Mehra, and Carlos Gutirrez. Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad-hoc networks. International Conference on Mobile Computing and Networks, 9(1), January 2008.
9. J. Broch et al., "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. Mobicom '98.
10. K.-W. Chin, et al., "Implementation Experience with MANET Routing Protocols," ACM SIGCOMM Computer Communications Review, Nov. 2002, pp. 49-59.
11. K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, andE.M.Belding-Royer, “Authenticated Routing for Ad HocNetworks,”Proceedings of IEEE Journal on Selected Areas inCommunications, vol. 23, no. 3, March 2010.
12. L. M. Feeney, "A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks," Swedish Institute of Computer Science Technical Report T99/07, October 2006.
13. M. Frodigh, et al, "Wireless Ad Hoc Networking: The Art of Networking without a Network," Ericsson Review, No. 4, 2010.
14. N. Patwari, et al., "The Importance of the Multipoint-to-Multipoint Indoor Radio Channel in Ad Hoc Networks" [measurements at 925 MHz] Proc. IEEE WCNC 2002.
15. Y.C.Hu and A.Perrig, “A Survey of Secure Wireless Ad HocRouting,” IEEE Security and Privacy, vol. 2(3), pp. 28-39, May 2004.
16. Y.C.Hu, A.Perrig, and D.B.Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,”Proc. MobiCom’02, Atlanta, GA, pp. 12-13 September 2002.
17. Patrick Albers, Olivier Camp, Jean-Marc Percher1, Bernard Jouga, Ludovic Me, and Ricardo Puttini. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. 2005.
18. Stephan Bohacek, Katia Obrazka, and Jaoa P Hespanha. Saddle policies for secure routing in communication networks. IEEE Conference on Decision and Control, December 2002.
19. S. Kurkowski, et al., "MANET Simulation Studies: The Incredibles," ACM SIGMOBILE Mobile Computing and Communication Review,

Vol. 9, Issue 4 (October 2008),pp. 50-61.

20. B. Karp and H. Kung, "Greedy Perimeter tateless Routing for Wireless Networks", *In Proceedings of International Conference on Mobile Computing and Networking*, pp. 243-254(2003)

21. Y. A. Huang and W. Lee, "Attack Analysis and Detection for Adhoc Routing Protocols," *In Proceedings of* International *Symposium on Recent Advances in Intrusion Detection*, pp.125-145(2004).

22. L. Zhou S. B. Fred, and R. Van Renesse, "COCA: A Secure DistributedOnline Certification Authority", *ACM Trans. On Computer Systems*, Vol. 20, No. 4, pp. 329-368(2002).

23. M.Gasser and E.McDermott, "An Architecture for Practical Delegation in a Distributed System", *In Proceedings of IEEE Symposium on Security and Privacy*, pp. 20-30(2004).