International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10685-10695

http://www.ripublication.com

A Novel Technique Against Selfish Node Attacks

Bommisetty Meghana and Supriya M

Department of Computer Science & Engineering
AmritaVishwa Vidyapeetham, Bengaluru, Karnataka, India
meghana14377@gmail.com
Department of Computer Science & Engineering
AmritaVishwa Vidyapeetham, Bengaluru, Karnataka, India
m_supriya@blr.amrita.edu

Abstract

Mobile Adhoc Network (MANET) provides a huge cooperation between all participating nodes. Due to open medium and wide area networks usually there will be various vulnerable attacks which make various damages to the network topology and other activities of the network. The main contribution of the paper is to control various attacks and redesign the protocols in order to detect malicious and selfish nodes and provide cooperation through co-operative algorithm which provides centralized monitoring and management point. In the MANETs security is a very critical problem as the network is wide and open in nature, though many algorithms are designed in exhibiting the misbehaviors of nodes and controlling the curcial role of selfishness and trustiness. Due to open structure and very limited battery energy, some nodes may not cooperate correctly. This paper proposes a new Intrusion Detection System providing malicious node controlling, selfish node activities and trustiness and thus providing energy consumption activities. This approach also reduces energy consumption and controls energy hacking by moving the computation.

Keywords: MANET, Selfish nodes, Trusted nodes, IDS, Routing algorithm, Energy Consumption

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a wireless network and autonomous system providing communication with mobile hosts and devices connected by wireless links. The wireless transmission range of each node in MANET gets executed by multi-hop packet forwarding. Such networks are well established for various missions and critical applications such as communication, military operations providing enhanced communication and data sharing. As the MANETs are open, wide and large, there is

lack of authorization facilities and volatile network topology which makes it very hard to detect malicious nodes. All the mobile devices and hosts are battery powered and are with limited resources. In such a scenario, heavy weight security solutions are undesirable. In wireless networks, we have different types of malicious attacks that are to be identified and controlled. At the same time it is necessary to check the battery resources with selfish nodes and trusted nodes to provide enhanced security. This paper provides and deals with Denial of Service Attacks by a Trusted Node and Selfish node with emphasis on common attack which decreases the network performance.

Wireless networks follow many policies with various nodes forward needed with better policies controlling and providing Energy Activities with Trust and Selfish Nodes. The Activities depending on their user and node motivation can divides the nodes into three categories i.e., Firstly discussing about Malevolent Nodes which will not compromise the security of the MANET or other nodes. These node actions are directly or indirectly show the effect on their own maximization benefit. Secondly we discuss about selfish nodes which forwards other packets for maximizing their benefit with all expense by providing advantage to the same node. The final category discuss about trusted node which provides information of next consequent node status which are intentionally misbehaved or malevolent information about the nodes.

The energy consumption and energy attacks will intend to directly damage other nodes and the route. It also reduces the CPU cycles,battery life with available network bandwidth to forward packets in a secured and safe way. Since the selfish node need to preserve their own resources, we extend the selfish node with trusted node while using various services of others and consuming their resources and other energy of the nodes. In this paper we provide detecting routes and forwarding data packets with concept of energy consumption using trusted node and also consumes CPU time,energy, network-bandwidth and memory. Therefore there is a very strong motivation for each node to deny packet forwarding to other nodes based on the trust activity of the corresponding node and at the same time we also control the energy activities for all the nodes. According to the proposed attacking algorithm or technique the selfish and trusted node can be defined in three different ways.

Firstly, we take all the nodes participation in route discovery and route maintenance providing acceptance and refuses of forwarding data packets to its corresponding nodes. Secondly, we provide various route discovery activities in data forwarding with the acceptance of the node in pre finding the trust activity of its corresponding node and provide effective resource controlling and transmission of data packets in secure way. Finally, the node can behave better with safe energy levels providing various threshold between different nodes and controlling energy level falls which behave like node.

One of the immediate effects of node misbehavior activity and failures in wireless ad hoc networks is the node isolation and communication problem, due to which the perfect communication between nodes are completely dependent between nodes in throughout on routing and forwarding packets. The presence of selfish and trusted node is a direct cause for node isolation concept and network partitioning technique, which further affects network survivability and usage among the interconnected nodes. This paper traditionally discuss about node isolation, a novel

phenomenon in which nodes have no(active) neighbors. Hence, we will show that due to the presence of selfish node, a node can be isolated even if the presence of active neighbors [2].

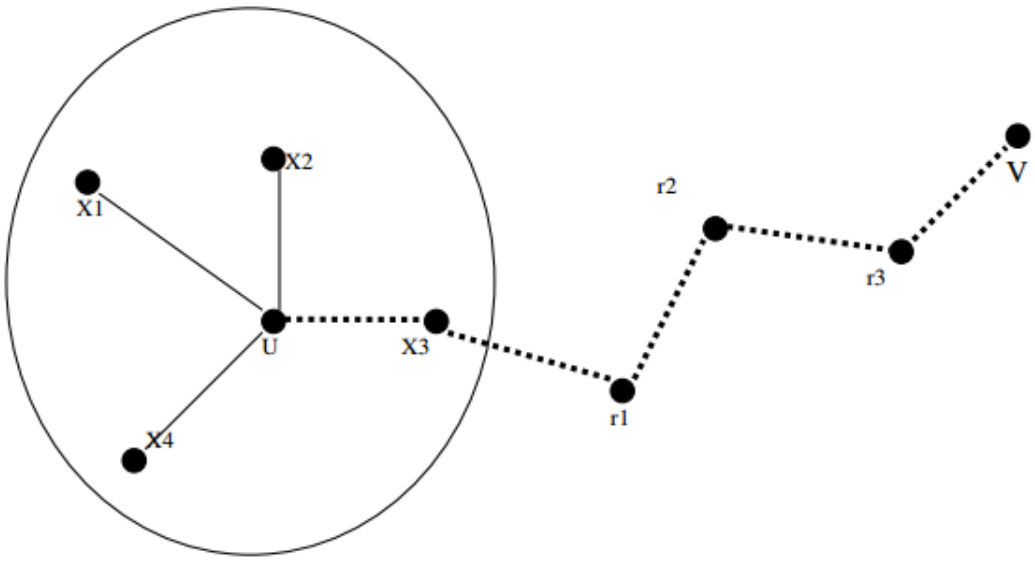

Fig 1: A hybrid MANET with routes to/from the gateway: very few nodes (grey) actually have to forward other nodes' data.

In Fig.1, we show Node x3 is suppose to be a selfish node where node u shows and initiates a route discovery to the corresponding node v. The selfish neighbors x3 may be reluctant to broadcast the information to the route request from the node u. In the proposed case x3 is a failed node and it is possible for x3 node to control packets. Since the proposed situation is very worse the u node may select x3 node as the next corresponding hop to send data to it. Consequently the x3 node may discard all the data packets via it and the communication between u and v cannot proceed. Here we discuss the issue when all the corresponding neighbors of u are selfish, the node u is unable to establish a secure communication with other nodes at proposed distance having more than one hop away. In the proposed case, we say that the entire node is to be isolated by its selfish neighbors.

Now we discuss and describe various possible attacks on MANETs. Various MANETs and its protocols have general attacks which are to be discussed before providing the project security activities. Coming to Passive Attacks like simplest attack on wireless network, which is a category of eavesdropping attack, a very minimal preparation is required but cannot be detected and this category is subdivided into content communication attack and infra structure meta data attack includes a attack on protocol and the attack reduce energy resources of node. Various amount of communication with identifying location and content can still be detected with traffic

patterns among the nodes.

When discussing about policy activities of MANET which disclose the information and location node's information might be considered a successful security breach and a node could not simply refuse to forward other node's connection when it is treated as un trusted node and we have two alternatives one the node not responding to route request is selfish behavior but not having impair in the net as suboptimal activities are found in the route. When the node does not respond to route request we discard the data which is it be forwarded to other node and eliminates the trust activity.

When discussing about active attacks where denial of service and enough resources on attacker is processed to destroy the energy activity of the node, that node cannot communicate with other nodes. Especially for mobile devices or clients they are vulnerable to denial of service attacks because their energy reserves are fastly drained off. Here we also have another possible approach to send large data to particular node and making the node energy drain and make the node to sleep. Direct attacks drains the energy and manipulates data activities.

When we discuss about Black hole attack where a node route is diverted to longest route and changes the shortest path to longest path disturbing existing routes so that more energy and time is used in transmission of data, traffic is increased and energy is consumed. This also leads to dropping of packets which is also called grey hole attack or various other attacks on traffic and its contents. Another attack is Sybil attack in which one malicious node is simulated with number of Independent nodes where the basis of log of maniupations are done on routing decisions distributing the route activities.

II. LITERATURE SURVEY

Several methods proposed to defend these attacks and we have studied various related work for reference of designing a novel and advanced selfish and trusted technique. The survey is described below.

Farooq Anjum et al. [1] proposed a new approach in detecting intrusions in mobile and ad hoc networks. Normally reactive ad-hoc routing protocols suffer from a very critical issues that is it is difficult to find intrusions. Detecting intruders will be more harder by the mobility.In this paper the probability of detecting an intrusion and the number of nodes participating in the process of detecting intrusions are analysed. Anand Patwardhan et al. [2] proposed a new secure routing protocol for AODV over Internet Protocol Version 6 (IPv6) and further enhanced by a routing protocol with independent activity of intrusion detection and automatic response system for mobile Ad hoc networks. Security in the routing considers the mechanism taken for non-repudiation and authentication, without having the availability of a Certificate Authority (CA) or a Key Distribution Center (KDC). Chin-Yang Henry Tseng [3] proposed full distributed intrusion detection with four new activities for MANET which has self reasoning activities. The distributed intrusion detection system detects all unknown attacks. The intrusion detection consists of AODV (Ad hoc On-demand Distance Vector) and OLSR (Optimized Link State Routing). This are used in MANETS for routing purpose. Distributed Evidence-driven Message Exchanging

intrusion detection Model (DEMEM)and Distributed Routing Evidence Tracing and Authentication intrusion prevention model(DRETA) are other activites provided. The main disadvantage is if the attacks increase in more number then the communication may breakdown at any time between the systems. The attack can be viewed in different ways by the users. Tarag Fahad and Robert Askwith [4] provided detection activities and conservation monitoring algorithm for detecting selfish nodes in MANETs. PCMA(packet conserving and monitoring algorithm) is generated for detecting the misbehavior of nodes and also defined partial dropping attacks and assuming some threshold value for this scenario.

Panagiotis Papadimitratos and Zygmunt J. Haas [5] proposed cryptography secure message transmission protocol with single path transmission and automatic configure to avoid transmission failures. The disadvantage is only cryptography would not work good for the wireless networks.

III. MOTIVATION

The main motivation for our work is to reduce the limitations of current IDS systems and address a new novel technique in providing advantage of the mobile device paradigm. Here we address and show solutions to various limitations which are earlier proposed and having some defects we show selfish routing with trust node management and energy controlling to reduce the false positive rate and provide a good reputation based scheme for increasing the network performance and scalability. The proposed technique shows good scalability for centralized approach in reducing Intrusion attacks on routing, between nodes and energy activities. By using Mobile Agent the scalability may increase that enhance the network performance. As the MANET is open medium and wide area which requires centralized controlling but due to various other components in local exchanging it is not able to secure centralized authorization of previous IDS the IDS cannot perform efficiently.

IV. PROPOSED WORK

The main objective of the projected work is to find the malicious nodes and improves the performance of nodes, network by selfish and trusted routing network. The assumptions regarding the proposed work are listed below

1. We construct and interact with 1 to many hop neighbors directly with intermediate nodes using multi hop packet forwarding.
2. Here all the nodes will have unique id in the network which is automatically assigned to the existing nodes.
3. We generate and transmit message from source node and sends to router.
4. The router moves the information towards shortest path controlling selfish activities with trusted routing and controlling energy activities and discovers a malicious node, instead of moving forward, it sends a report to the source node.

   In Fig 2 we show the data transmission between node 1 and node 10 where node 1 is source node and node ten is destination node and considering neighbor list 3,4,5,8 and 9 shown in Table 1.

Table 1: Neighbor Nodes Information

Node ID	Neighbors
6	3,4,5,8,9

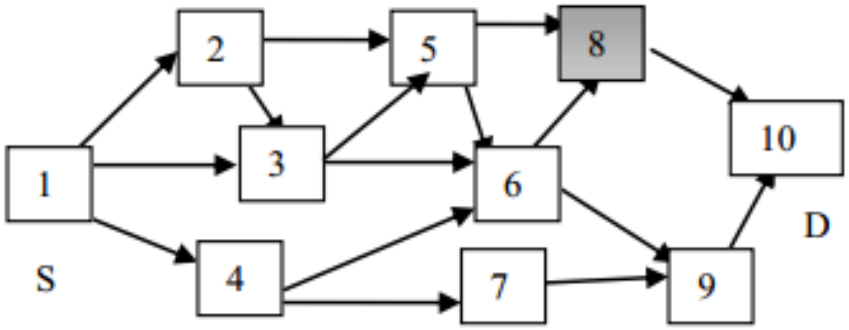

Fig 2: A MANET of 10 nodes

The above figure shows various neighbor nodes to send and receive the message from source to destination to see if it is the intended recipient. If yes it sends a message to the next consequent node and the current sequence of route node 3, 4, 5, 8, 9 maintain the sequence number in the SnT and sequence numbers are generated randomly in simulation shown in Table 2.

Table 2: DST Sequence Information

Node ID	DST_Seq
3	10
4	7
5	8
8	6
9	5

When an intermediate node receives a message it checks if the difference between the Dst node and Seq node to present in the route for transmitting a message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as “M” or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node’s id and neighbor list of the malicious node. Node 6 keeps track of the status of each neighbor node in the ST whether it is a safe node or a malicious one. Suppose we consider node 8 as malicious. The ST is shown in Table 3.

Table 3: Status Table Information

Node ID	DST_Seq
3	S
4	S
5	S
8	M
9	S

The neighbor nodes of node 8 are 5, 6, 10.Then these nodes after receiving the Further Detection message, broadcast a requested message by setting destination address to source node's address. If it receives a requested message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route. Then the source node waits for "wt" time until it receives the entire test and acknowledgement packet. If, SN receives a TP, it updates the Flag Table (FT) by adding the source node id to the table and set the flag of the node as "Y" and if an AP is received set the flag as "N" and update the count field. Table 4 shows the Flag Table maintained by node 1 is as follows:

Table 4: Flag Table

Node ID	DST_Seq
5	N
6	N
10	N

If all the entries for the malicious node are "N" then source node updates the status table (ST) by adding the MN's id to the ST and making the status as "B" i.e. Black hole. After confirmation of the Black hole node the ST of source node 1 is given as B in table 5.

Table 5: Flag Table consists of black hole

Node ID	DST_Seq
7	B

V. ALGORITHM FOR ROUTING FROM SOURCE TO DESTINATION NODE

Step 1: The source node N_0 sends packet to the destination node N_6

Step 2: Start Timer T.

Step 3:Wait for the acknowledgement from destination node.

Step 4: Increase T by unit time.
Step 5: If T>Tout then
Goto step 6
Else
Goto step 3
Step 6: The Source node generates Mobile Agent(MA) and provides it's own ID and send it to the next hop node
Step 7:The mobile agent observe for i^{th} node the number of
Packets are received from node j neighbor and compute CPR(i,j)
Step 8: MA compute CPF(i,j)for the i^{th} node
Step 9: MA compute Pdr(i,j) for the i^{th} node at t^{th} instance
Step 10: If the pdr is less than threshold value which is approximate for i^{th} node
Then
The node moves to the next hop node and decrease hop count by 1
Else
Node reports the selfish node or malicious activity to the source node
Finish

VI. PERFORMANCE ANALYSIS

The projected is system provides better performance of network routing, energy saving, selfish controlling and trusted routing by comparing the performance of old system we can say the simulation metrics shows better result and observation with enhanced performance of the network in presence and controlling the malicious nodes. The presence of mobile network performance we can improve the network by preventing malicious nodes. Initially the Average Throughput of Receiving Packet is same implies that the network is free from network at that instant time. The packet size increases the throughput is about to decreases means due to packet overhead the throughput decreases.

The existing system which is compared with our proposed system is the SCF (Self Centred Friendship) tree [6].This existing system is named as IDS1 in our paper. SCF tree based system finds only the selfish nodes which are detected by using the depth first search. The main step in this existing method is building a SCF tree for each node in the network. Here selfish nodes are identified by using the credit risk(CR) value. If the value is greater than threshold value then it is considered as selfish else not. The main drawback here is, if any attacks are observed then this cannot be detected by this existing system. But in our proposed system we can detect IDS attacks, selfish nodes and other attacks. This section compares the SCF tree based method called IDS 1 and our proposed method called IDS 2 using various graph representations.

The Fig 3 show the routing analysis in case of IDS attack. Here we can observe the effect of attack. If there is attack only some packets are delivered and all the other packets are droped by selfish nodes then NRL is minimum. In the fig 3 we consider selfish as IDS1 and proposed work as IDS2.But by applying IDS a secure routing packet also deliver successfully data between the nodes.

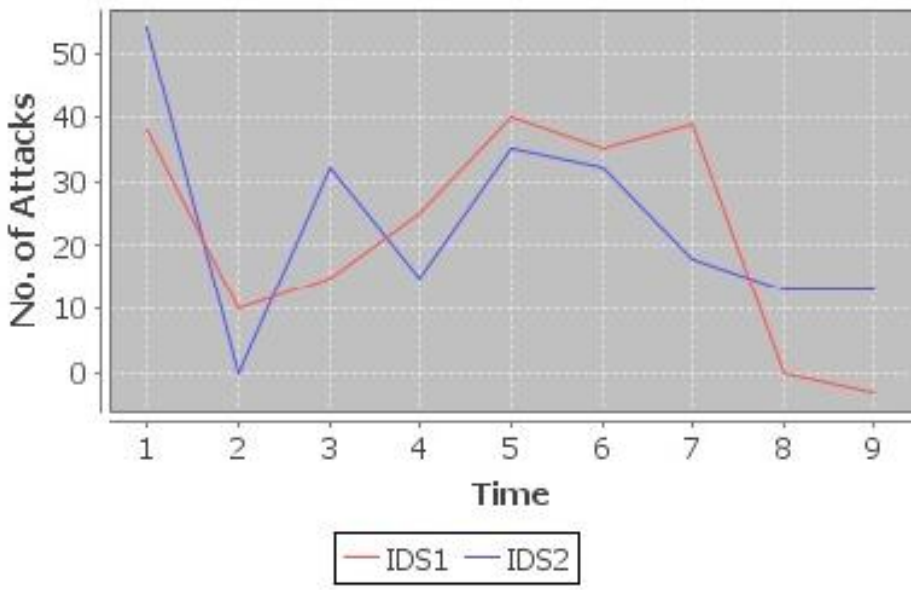

Fig 3. NRL analysis in case of IDS attack

The Fig 4 shows the throughput analysis comparision for the selfish and IDS with attacks. In the case of IDS1 which denotes the selfish nodes the throughput is very less with the attacks being increased IDS2 the proposed results are better than the selfish as attacks are increasing also the time taken to detect is less than the IDS1.IDS2 sends more packets in the presence of many attacks.

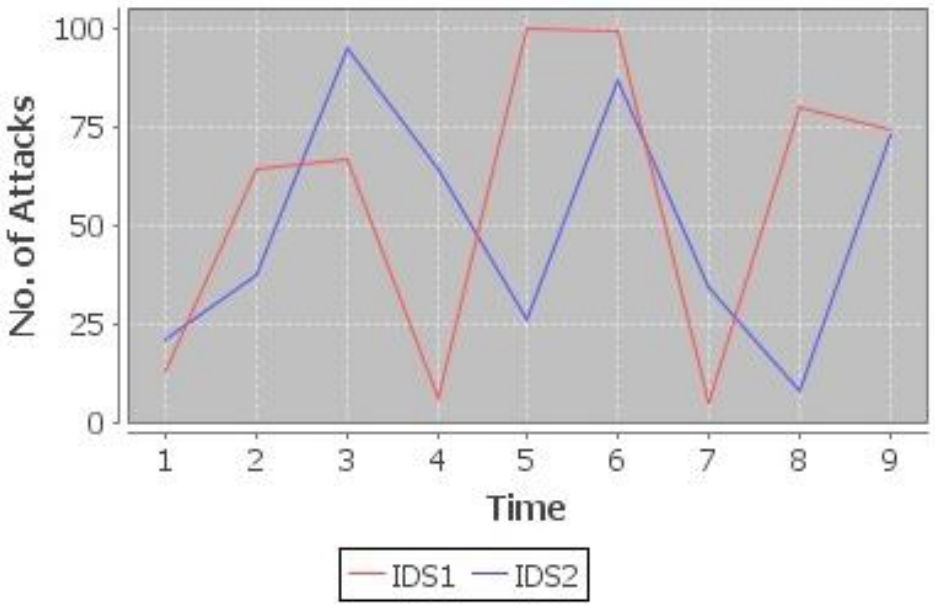

Fig 4: Throughput analysis in case of IDS attacks

The Fig 5 shows the packet delivery ratio with the attacks and the time taken for delivering the packets in the presence of attacks. Here we can observe that packet delivering is more in the IDS2 proposed system with the attacks been increased also. Thus the IDS2 proposed system is better than the others since packet delivering also increased with the number of attacks been increased also.

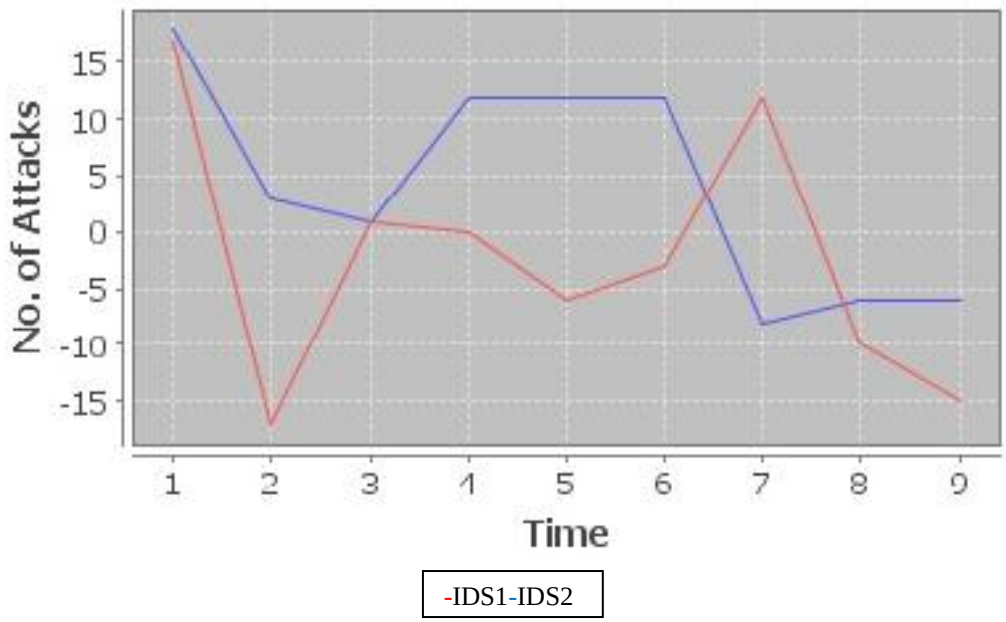

Fig 5: PDF analysis in case of IDS attacks

VII. CONCLUSION AND FUTURE SCOPE

We can conclude that mobile ad-hoc network are suffering from various types of intrusions, denial of service attacks by selfish node. In wireless networks especially in mobile Ad Hoc networks a mobile agent will be traveling through the network gathering various vital information, as open medium and large networks we have many thresholds and attacks on energy, route and other activities of the network. The work proposes a novel technique with computation complexity and minimizes overhead by controlling various attacks and reducing the refusing of packet delivery among the neighbor nodes. The nodes are also free from performing the computation. The future of our proposed scheme is to increases the efficiency of each node and thus it increases the overall performance of the network.

REFERENCES

[1] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "*Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols*" in proceedings of IEEE 58th Conference on

Vehicular Technology, 2003.

[2] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "*Secure Routing and Intrusion Detection in Ad Hoc Networks*" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

[3] Chin-Yang Henry Tseng, *"Distributed Intrusion Detection Models for Mobile Ad Hoc Networks*" University of California at Davis Davis, CA, USA , 2006.

[4] Tarag Fahad and Robert Askwith "*A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks*", in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[5] Panagiotis Papadimitratos, and Zygmunt J. Haas, "*Secure Data Communication in Mobile Ad Hoc Networks"*, IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006. [6] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.

[6] Jae-Ho Choi, Kyu-Sun Shim, *"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network"* SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE.2012