International Journal of Current Trends in Engineering & Technology
Volume: 02, Issue: 01 (JAN-FAB, 2016)

Sybil Attack Multiple Identification Security Mechanism in MANET

Priyanka Patware [1], Prof. S. R. Yadav [2]
MITS, Bhopal, India
[1]priyanka.patware59@gmail.com, [2]techmillenniumk.yadav@gmail.com

***Abstract*—The mobile nodes in MANET (Mobile Ad Hoc Network) continuously move with different mobility speed. Due to that links between the nodes are created and destroyed in an unpredictable way, which makes quite challenging the determination of routes between a pair of nodes that want to communicate with each other. The attacker presence in network is another one challenge. The Sybil attacker is the routing layer active attacker that replies with multiple identification number to nearby nodes. The Sybil attacker forward request in a different time instant and drop the data forwarded to attacker after link establishment. The proposed research work is provides the novel security mechanism against routing misbehavior of Sybil attack in MANET. The proposed existing security scheme will detect the attack identification in network and block their whole misbehavior activity. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is not comparable to normal losses. The attacker loss is more than the other losses like collision and out of range. The proposed security mechanism is detecting attacker node that reply with multiple security mechanism and broadcast the particular attacker original identity that generate fake identity. Therefore, by detecting the malicious or attacker loss percentage is decided whether the packet loss is purely due to a combined effect of fake. The attacker detection is confirmed by TPR and FPR. The proposed security scheme is improves the routing performance and blocks the attacker existence in network.**

***Keywords*— Sybil attacker, MANET, Security, Routing, Multiple Identities.**

I. INTRODUCTION

In some situations when there is an urgent need for network communication between collection of hosts in absence of centralized administrator and fixed infrastructure are unavailable or difficult to deploy that means it is time for mobile ad hoc network. MANET [1] has many characteristic which make it suitable for some important applications and it can provide services well in such cases. Mobile ad hoc network have become an important part of our life due to its vital services which provided to the population and society. It used at home, work, emergency situation, and natural disaster. On the other hand, the threats of MANET have flourished too. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. There are several types of attacks and intrusions targeting wireless networks as general especially mobile ad hoc network because of the nature of its work [1]. These attacks directly affect the performance and the survivability of MANETs. There are many efforts have done to surviving MANETs and keep them to provide services even in the presence of intrusion and attacks. Figure 1 represents communication between the nodes in MANET environment.

Fig. 1 Mobile Ad hoc Network

Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories, first is routing disruption attack which the attacker trying to change the course of packets. Second resource consumption attack, the attacker inserts packet into the network to consume resources [2]. Attacks on MANET are classified as Active and Passive attacks [3], passive attacks are not dangerous if the delivering data is important than its security, because it does not affects the normal operation of MANET, while active attacks affecting the normal operation of MANET In several ways. This survey focusing on initiatives which make MANET survives against active attacks. Malicious node causes packet dropping, false routing and etc. Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- No intention for bandwidth utilization.
- Launch all kinds of attacks replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages but their attack mechanisms are different.

II. ROUTING IN MANET

According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing [4, 5].

A. Proactive (table-driven) Routing Protocol

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbor's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol and Optimized link state routing (OLSR) protocol.

B. Reactive (on-demand) Routing Protocol

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: - Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP)

III. LITERATURE SURVEY

The attackers are degrades the network performance at different layers. In this survey we focus on the misbehavior of Sybil attack in MANET.

Authors (Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat) [6] “Lightweight Sybil Attack Detection in MANETs” in this title we discuss a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

Author (Nitish Balachandran) [7] “A Review of Techniques to Mitigate Sybil Attacks” In this title, we discuss the different kinds of Sybil attacks including those occurring in peer-to-peer reputation systems, self-organizing networks and even social network systems. In addition, various methods that have been suggested over time to decrease or eliminate their risk completely are also analyzed along with their modus operandi.

Authors (Chris Piro Clay Shields Brian Neil Levine) [8] “Detecting the Sybil Attack in Mobile Ad hoc Networks” In this title, we show that mobility can be used to enhance security. Specifically, we show that nodes that passively monitor traffic in the network can detect a Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. We then show that although the detection mechanism will falsely identify groups of nodes travelling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes travelling in close proximity.

Authors (Sarosh Hashmi, John Brooke) [9] “Towards Sybil Resistant Authentication in Mobile Ad hoc Networks” In this tile we present an authentication mechanism for MANETs that utilizes hardware id of the device of each node for authentication. An authentication agent is developed that verifies the hardware id of the authenticate node. A comprehensive defense model is employed to protect the authentication agent from various static and dynamic attacks from a potentially malicious authenticate node. Security of authenticate node is assured by involving a TTP that signs the authentication agent, verifying that it will perform only intended function and is safe to execute. With this minimal involvement of the TTP, the proposed authentication scheme offers increased resistance to the Sybil attack. The attacker is now required to either thwart agent protection mechanisms or to acquire multiple devices with different hardware ids, in order to gain multiple identities.

Authors (Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial) [10] “Sybil Nodes Detection Based on Received Signal Strength Variations within VANET” We present in this context a Sybil detection approach, based on received signal strength variations, allowing a node to verify the authenticity of other communicating nodes, according to their localizations. In addition, we demean estimated metric of the distinguish ability degree between two nodes, allowing to determine Sybil and malicious ones within VANET. The applicability of our contributions is validated through geometrical analysis, simulations and real measurements.

Authors (James Newsome, Elaine Shi, Dawn Song, Adrian Perrig) [11] “The Sybil Attack in Sensor Networks: Analysis & Defenses” This title systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. We demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. We establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design countermeasures against each type. We then propose several novel techniques to defend against the Sybil attack, and analyze their electiveness quantitatively.

IV. PROPOSED WORK

The problem of multiple identities is degrades network performance by that we focus on to detect Sybil attack and protect against that attack, so first we deploy Sybil attack scenario in two ways same time more identification and scenario -2 different time different identification and both case we deploy reputation-based protector system. In our Sybil attack scheme, we will consider both types of Sybil attacks. The strategy of our detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks. Hence, in this thesis, we will refer to the new Sybil identity and whitewash identity where they completion of data receives or simulation end. We assume that the attacker joins the network with its single identity, and that malicious nodes do not collide with one another. We also assume that nodes do not increase or decrease their transmit power. The attackers can get identities by two ways. First, they can fabricate identities (Second, they can use stolen identities, i.e., spoof the identities of legitimate nodes (masquerading) in the network. We assume the first case where nodes can create arbitrary identifiers because in MANETs, there are no restrictions on identity creation. After attack module we generate profile table during simulation and apply IP header checking base technique through abstract window tool kit and detect misleading node and number of packet captured by the Sybil attacker node in both scenario. And lastly we design reputation-based, protection system in that system check all neighbour node IP address and if any node adversely sends different identification into more than two different sender so protector nodes is identify that particular node and more than one protector node collaboratively make decision for blocking that path and true information all sender node so they cannot sends any data through that attacker node.

A. Proposed algorithm

The Here we define algorithm for how the Sybil attack spread onto the network, basically according to definition number of different way Sybil attack spread into the network There are two flavours of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any wrong history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack and defines through algorithm bases very first we set normal ad-hoc network parameter and set criteria of Sybil attack scheme and spread attack onto the network.

```
    Number of Nodes = $M_N$;    // Mobile Nodes
    Number of Sender Nodes = $S_n$;    // $S_n$ € $M_N$ ;
    Destination Nodes = $D_n$;  // D € $M_N$;
    Routing Protocol Considered = Reactive (AODV);
    Set Simulation Time = $T_t$    // taken $T_t$= 100
    Set Radio Range = RR of $M_N$;    // Initialize Nodes Radio Range
    Set Sybil Attcaker = $S_n$;
    $S_n$_RREQ_B ( D, RR )   // broadcast RREQ for nodes that are in range.
            {
    If ((RR<=550) && (next hop >0))
            {
            Forward Route Request;
            {
     rtable->insert(rtable->rt_nexthop);  //  nexthop  to  RREQ source
            if (next_hop = = destination )
            {
            Store minimum next_hop(S,next_hop,D)
            Minimum_hop_rtable=rtable;   //RREP   Sends   via shortest link//
             }
            Else
            {
            Send ACK to source $S_i$ by $D_n$ node entered in rtable1;
            Data_packet_send (s_no, nexthop, type)
            }
else
            {
            Destination not found;
            }
}
}
```

Attacker Detection and Prevention

```
{       // Sybil Node spread route misbehaver module ;
 Set Sybil node = $S_n$; // $S_n$ Sybil Attacker Node
 If ($S_n$ in radio range && active)
{
        Update routing Table;
        Set $D_n$_id = Self_id ($SA_n$);
// Mis identification
        Increase Hop count++;

        Send $SA_n$ certainly RREP to $S_n$;
        }
        Data_packet_send (s_no, nexthop, type)
           {
        if (Data forwarding from  $SA_n$ == Pessimistic)
        {
        Capture data $SA_n$;
        Block that particular $SA_n$ nodes;
        }
        Else
        {
        forwarded data packets no attacker exist
         }
         }
else    {
        destination un-reachable ;
      }
}
}
```

V. SIMULATION ENVIRONMENT AND RESULT DISCUSSION

Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [12]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol. The simulator is written in C++ and a script language called OTCL2. Ns use an OTCL interpreter towards the user. This means that the user writes an OTCL script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

A. Simulation Parameters

The some simulation parameters mentioned in table1. These parameters are also change based on requirement so, this table only gives the estimation of it.

Table -1 simulation parameters

Number of nodes	30
Dimension of simulated area	800×800
Routing Protocol	AODV
Simulation time (seconds)	100
Attack Module	Sybil Attack
Transport Layer	TCP ,FTP
Antenna Type	Omni Antenna
Traffic type	CBR,FTP
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	Random

B. Performance Evaluation

There are following different performance metrics [4] has been considered to make the comparative study of these routing protocols through simulation.

1) **Infection Rate:** Rate of infection in network w. r. t time.
2) **Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent to propagate the data packets.
3) **Average Delay:** This metric represents average end-to-end delay and indicates how long it took a packet to travel from the source to the application layer of the destination. It is measuring in mille seconds.
4) **Throughput:** This metric represents the total number of bits forwarded to higher layers per second.
5) **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

C. Packet Delivery Ratio

The Packet delivery ratio is very important parameter for data analysis in network communication because that parameter gives the information about percentage of data receiver by the receiver out of actual data packet sends by the sender, here we analyze that packet delivery value and evaluated in normal network as well as in Sybil attack scenario and proposed protection system. The percentage of data receives is nearly 9 to 92 percent up to end of simulation in normal routing and proposed secure routing in presence of Sybil attacker but Sybil attack1 and Sybil attack2 has shows the performance degradation in the whole network. The PDR performance in presence of attacker is in scenario reaches from 23% to1% is negligible mark but reaches to 55 % at the start of Sybil attacker 2. The performance of scenario-2 is also same maintain3ed at 10 % as one except the end time simulation performance.

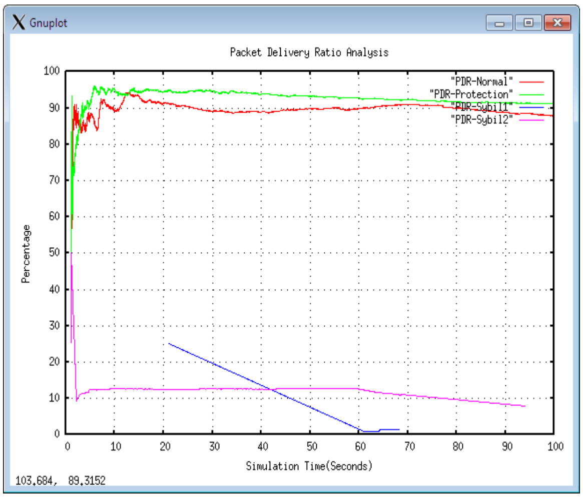

Fig.2 PDR Analysis

D.Routing Load Analysis

The sender is flooding the packets in network for finding the destination. Every node in network is forwarded the routing packets in network till the destination is not found. In this graph we analyze our routing overhead in case of normal time, attacker and security scheme but both Sybil attack scenario routing overhead is lower because if sender search actual receiver and same time any nearby of Sybil attacker is present that certainly gives the misidentification number of receiver and route reply message send to sender by receiver. In that case actual sender cannot search any of the paths and actual data packets are dropped by attacker. The routing packets in normal and proposed security scheme are high but data receiving is also high with minimum overhead.

E. Attack Data Loss Percentage

The attacker in network is degrading the whole routing performance by that the network performance is drastic effected. Sybil attack is very big challenge in MANET environment because trustiness is very essential requirement for Ad hoc network, without the trust we cannot search actual receiver node, and that situation if any node spread Sybil attack our all data receives by mislead node, in that graph we shows two different situation and analyze the data receives percentage by the unauthorized user, in scenario-1 if different time node gives different identification and scenario-2 same time gives more than two identification and found both case about 50% and 40% data receives by malicious nodes.

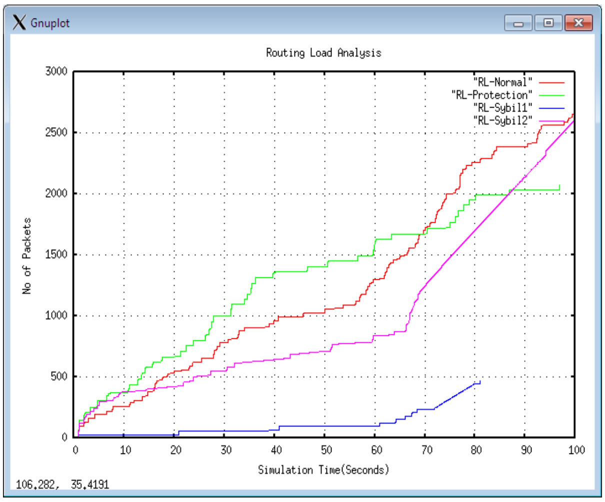

Fig.3 Routing Packets Analysis

F. False Positive Detection

False positive it means wrong detection, where node is normal but behaves like abnormal or attacker, while false positive is greater it means detection mechanism not correctly identifies or separate between the attacker or normal nodes. In this graph shows that false positive analysis in both Sybil attacker scenario and identifies that scene 2 case initial time 7% normal node treat like attacker because their behaviour as a Sybil attacker, but average case nearly 6% and the scene1 Sybil case nearly 2% till the 75 seconds and after that the percentage is 65, here false positive value is less than 10% so that is considerable for detection process.

G. True Positive Detection

In the Sybil attack scenario, attacker node is gives false identification for gaining network resources and data from sender nodes. True positive is a mechanism to positively detection (node really misbehave and identifies them) of attacker nodes with the help of available information of sending and receiving data in network.

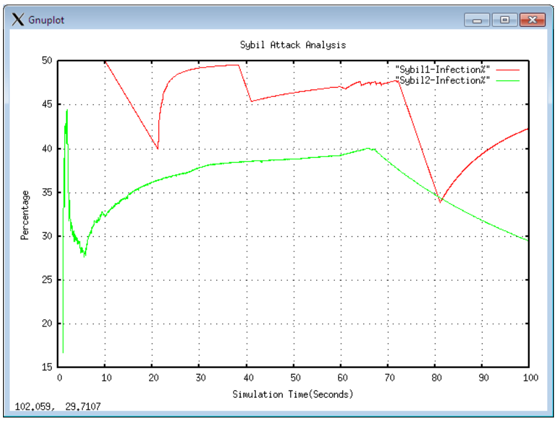

Fig.4 Attacker Loss Percentage Analysis

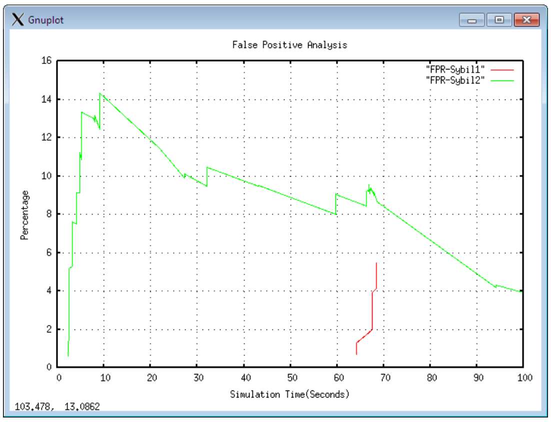

Fig.5 FP Detection Analysis

In this graph shows that Sybil attack in the network in same time as well as different time and analyze that both Sybil scenarios greater than 80 percentage of truly attacker detected.

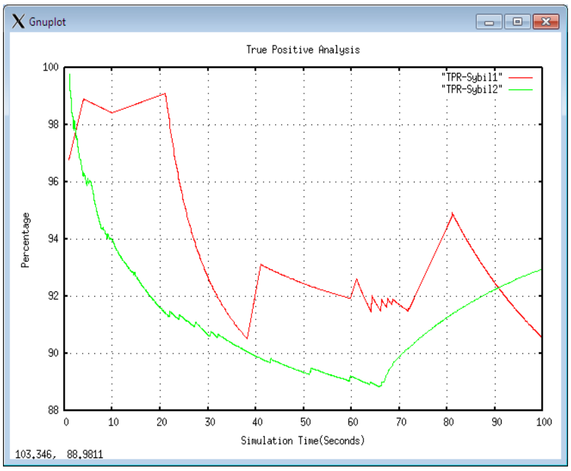

Fig. 6 TP Detection Analysis

VI. CONCLUSION & FUTURE SCOPE

Mobile Ad hoc Network (MANET) are liable from routing attacks due absence of centralized monitoring and management, so it is crucial to protect them. Sybil attack, an attacker node behaves as if it were a group of nodes by showing multiple Identities in network. There are, basically two ways by which a Sybil attacker node/s can be possible to get an identity of other nodes i.e. by abducting other normal node's identity and creating false identities itself. In this research we use the second way to identify the Sybil attacker in network. Routing protocol independent attacks are not prone to occur for specific routing protocol this attack can take place irrespective of the routing protocol. The routing protocol dependent attacker identification is basically limited and for other routing protocol identification is not possible. The main advantage of proposed security scheme is it is protocol independent .The proposed security mechanism is identified the false identity information of attacker and improves the routing performance of network in presence of attacker. The security mechanism improves the throughput, PDF, FPR and reduces routing load, packet dropping, reduces TPR value in presence of attacker and IDS nodes. The proposed security mechanism completely removes malicious drop percentage that confirms the no attacker existence of attacker contamination and provides attacker free secure routing in MANET. The future scope of this research is to identify the other attacker like wormhole attack and remapping attack on the basis of attacker identification and also try to work on the dynamic topology control system. In This scheme we observe higher mobility of mobile nodes and forward the message to control their mobility to reduce the chances of link in network and the second option is to try to ignore that nodes selection in routing.

REFERENCES

[1] Macro Conti, Silvia Giordano and Ivan Stojmenovi "Mobile Ad Hoc Networks", Stefano Basagni, IEEE press, A john Wily & Sons, INC. publication, 2003

[2] A.K. Rai, R. R. Tewari and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security, Vol. 4, No. 3, 2010, pp. 265-274.

[3] B. Wu, J. M. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, Berlin, pp. 103-135, 2007.

[4] Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285, August 2010.

[5] Ipsita Panda "A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012

[6] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat "Lightweight Sybil Attack Detection in Manets" IEEE Systems Journal, Vol. 7, No. 2, June 2013.

[7] Nitish Balachandran "A Review of Techniques to Mitigate Sybil Attacks" Int. J. Advanced Networking and Applications 11 July 2012.

[8] Chris Piro Clay Shields Brian Neil Levine "Detecting the Sybil Attack in Mobile Ad hoc Networks" NSF grants CNS-0133055, CNS-0534618, and CNS-0087639.

[9] Sarosh Hashmi, John Brooke, "Towards Sybil Resistant Authentication in Mobile Ad hoc Networks" 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies.

[10] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET" International Journal of Network Security, Vol.9, No.1, PP.22-33, July 2009.

[11] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses" IPSN'04, April 26–27, 2004, Berkeley, California, USA.

[12] http://www.isi.edu/nsnam/ns/.