International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 02 (March - April, 2017)

An Identity Based Pervention Scheme Using IDS Against Sybil Attack in MANET

Nidhi Jain
M. Tech. Scholar
Department of CSE
BERI, RGPV, Bhopal, M.P., (India)
nidhi_jain2004@yahoo.com

Dr. Tripti Arjariya
Department of CSE
BERI, RGPV, Bhopal, M.P., (India)
tripti.beri@gmail.com

Dr. Mohit Gangwar
Department of CSE
BERI, RGPV, Bhopal, M.P., (India)
mohitgangwar@gmail.com

***Abstract*—**Mobile Ad hoc Networks also called in short (MANET) are a group of nodes which are independent and connected with each other through wireless connection. Through specific routing protocol like AODV nodes communicate with each other by interchange of packets. The routing packets are consider for connection establishment and data packets are the actual data sending by sender to destination after connection establishment. Nodes in MANET are create dynamic structure because of they are continuously moves in network. Those nodes which are not in wireless range reach to hop by hop through these nodes in network. Due to lack of a defined essential authority, secure the routing becomes a challenging task. In this paper we proposed the security against Sybil attack to secure network from malicious nodes. Malicious nodes are creating the multiple identifies in network by capturing other nodes identification (Node Number) and communicate with other nodes through fake ID. By doing this, the malicious node can deprive the traffic from the source node. The proposed security scheme is continuously watch the attacker malicious functioning in and also find the fake ID of attacker because every fake ID is performing malicious functioning. The security scheme identifies the attacker existence through False and True detection calculation and blocks the attacker malicious functioning in MANET. The proposed security approach is improves network performance and provides secure routing in MANET.

***Keywords*—** MANET, Routing, Sybil attack, misbehaviour, Security, packets dropping, Identification(ID) .

I. INTRODUCTION

Mobil Ad- hoc networks (MANETs) represent complicated a distributed system that contains wireless mobile nodes which will dynamically and freely self-organize into capricious and temporary unplanned network topologies [1]. This permits folks and devices to seamlessly internetwork in areas wherever no pre-existing communication infrastructure exists, as example disaster recovery environments. The distinctive characteristics of MANETs, like dynamic topology and resource constraint devices, create variety of nontrivial challenges for economical and trivial security protocols style. In figure q nodes are communicate with each other in open environment. The every device which is battery dependent and having capability like sensor will be assume as mobile node in MANET. Due to the dearth of centralized identity management in MANETs and also the demand of a singular, distinct, and chronic identity per node for his or her security protocols to be viable, Sybil attacks create a heavy threat to such networks. As an example, communications in wireless networks are measure sometimes supported a singular symbol that represents a network entity: a node. Identifiers are measure used as associate degree address to speak with a network entity [2].

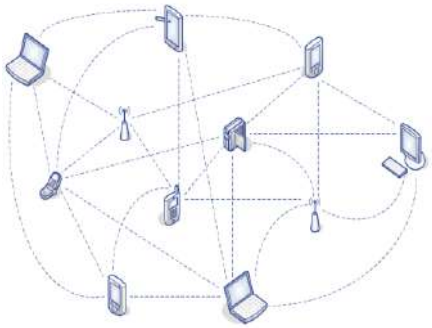

Fig. 1 Mobile ad-hoc Network

This forms a matched mapping between an identity and an entity which is sometimes assumed either implicitly or expressly by several protocol mechanisms; thus one identity implies two distinct nodes. Despondently malicious nodes will illegitimately claim multiple identities and violate this one-tone mapping of identity and entity philosophy. The term "ad hoc" implies that this network could be a network established for a special, usually ad-lib service made-to-order to applications. So, the standard unexpected network is ready up for a restricted amount of your time. The protocols square measure tuned to the actual application (e.g., send a video stream across the field; resolve if a fireplace has started within the forest; establish a videoconference among three groups engaged in an exceedingly rescue effort). The applying could also be mobile and also the atmosphere might amendment dynamically. Consequently, the unexpected protocols should self-configure to regulate to atmosphere, traffic and mission changes. What emerges from these characteristics if the vision of an especially versatile, malleable and nonetheless strong and formidable spec. associate degree design which will be accustomed monitor the habits of birds in their natural environment, and which, in alternative circumstances, is structured to launch deadly attacks onto unsuspecting enemies.

Because of its mobile, non-infrastructure nature, the unexpected network poses new style necessities. The primary is self-configuration (of addresses and routing) within the face of quality. At the applying level, unexpected network users usually communicate and collaborate as groups (for example, police, fire-fighters, medical personnel groups in an exceedingly search and rescue mission).These applications so need economical cluster communications (multicasting) for each

knowledge and real time traffic. Moreover, quality stimulates a number of location primarily based services nonexistent within the wired net. Routing protocols [3] of MANET are not same as wired or wireless routing protocols. These protocols are completely different and designed for dynamic network. In this research AODV (Ad hoc On Demand Distance Vector) [4] routing protocol is used for simulation.

II. Security Threats in MANETS

The present mobile ad-hoc networks give many various varieties of attacks. Though the analogous exploits conjointly exits in wired networks however it's simple to mend by infrastructure in such a network. Current MANET's are measure primarily prone to two differing kinds of attacks: active attacks and passive attacks [5]. Active attack is attack once misbehaving node needs to bear some energy prices so as to perform the threat. On the opposite hand, passive attacks are measure principally attributable to lack of cooperation with the aim of saving energy egotistically. Nodes that perform active attacks with the aim of damaging alternative nodes by inflicting network outage are measure thought of as malicious whereas nodes that build passive attacks with the aim of saving battery life for his or her own communications are measure thought of to be stingy. During this the attacks are measure classified as modification, impersonation, fabrication, hole and lack of cooperation.

III. Network Intrusion Detection Systems (IDS)

Network IDS historically include many modules an audit module, a detection module and a response module [6, 7].

1. Host-based, within which every node performs intrusion detection and might be any localized if they impart their detection outcomes to at least one another.
2. Hierarchical, typically utilized in heterogeneous networking environments, wherever device categories have procedure and memory constraints that impose a limit on their role within the overall IDS.
3. Fully centralized, wherever one device is answerable for providing IDS services for the whole network.

IV. Literature Survey

In this section we actually discuss the previous work done in field of security against Sybil attack and other identity based attack in MANET.

Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat [1] "Lightweight Sybil Attack Detection in MANETs" During this analysis, we tend to propose a light-weight theme to find the new identities of Sybil attackers while not using centralized trusty third party or any further hardware, like directional antennae or a geographical positioning system. Through the assistance of in depth simulations and real-world testbed experiments, we tend to area unit able to demonstrate that our planned theme detects Sybil identities with smart accuracy even within the presence of quality.

Athichart Tangpong, George Kesidis, Hung-yuan Hsu, and Ali Hurson [8] sturdy Sybil Detection for MANETs we tend to propose a sturdy Sybil attack detection framework for MANETs supported cooperative watching of network activities. We be liable to don't need selected and honest monitors to perform the Sybil attack detection. Every mobile node within the network observes packets passing through it and sporadically exchanges its observations so as to work out the presence of an attack. Malicious nodes fabricating false observations are detected and rendered ineffective. Our framework needs no centralized authority and, thus, is ascendible in increasing network size. Privacy of every mobile node is additionally a thought of our framework. Our preliminary experimental results yield on top of eightieth accuracy (true positives) and concerning 100% error rate (false positives).

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones [9] "Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks "during this title we tend to describe a name based theme for MANETs that acts as a deterrent for whitewashing attacks. Instead of making an attempt to find whitewashing attacks, we tend to approach the matter in an exceedingly novel means by removing the benefits that whitewashing will offer. In our planned theme, every node should pay an entry fee to consume network services. As financial fees don't seem to be appropriate for MANETs because of fee management complications, rather than a financial fee we tend to use a fee within the style of cooperation. A node can receive services from the network when it cooperates till its name is enlarged to a definite level Y. For a traditional egotistic node, it's not useful to perform a whitewash as a result of it'll be needed to pay the entry fee when it enters into the network. Simulation results show that our theme performs well in reducing attacker outcome and attacker nodes' utility as compared to the friend theme within the presence of whitewashing nodes.

Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE [10] "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks" During this title we tend to describe however we tend to integrated our attack detector into a time period indoor localization system, which might additionally localize the positions of the attackers. We tend to show that the positions of the attackers are often localized using either area- or point-based localization algorithms with an equivalent relative errors as within the traditional case. We tend to additional evaluated our ways through experimentation in 2 real workplace buildings using each AN IEEE 802.11 (WiFi) network an and IEEE 802.15.4 (ZigBee) network. Our results show that it's attainable to find wireless identity-based attacks with each a high detection rate and a coffee false-positive rate, thereby providing sturdy proof of the effectiveness of the attack detector utilizing the special correlation of RSS and therefore the attack localizer.

A.Rajaram. Dr. S. Palaniswami "Malicious Node Detection System for Mobile Ad hoc Networks" [11] during this title, we tend to develop a trust based mostly security protocol supported a MAC-layer approach that

attains confidentiality and authentication of packets in each routing and link layers of MANETs. Within the 1st section of the protocol, we tend to style a trust based mostly packet forwarding theme for police investigation and uninflected the malicious nodes using the routing layer info. It uses trust values to favor packet forwarding by maintaining a trust counter for every node. A node is disciplined or rewarded by decreasing or increasing the trust counter. If the trust counter price falls below a trust threshold, the corresponding intermediate node is marked as malicious. Within the next section of the protocol, we offer link-layer security using the CBC-X mode of authentication and coding. By simulation results, we tend to show that the planned MAC-layer security protocol achieves high packet delivery quantitative relation whereas attaining low delay, high

Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial [12] we tend to present during this context a Sybil detection approach, supported received signal strength variations, permitting a node to verify the believability of alternative human activity nodes, ac- cording to their localizations. Additionally, we tend to outline a calculable metric of the distinguish ability degree between two nodes, permitting to work out Sybil and malicious ones inside VANET. The relevance of our contributions is valid through geometrical analysis, simulations and real measurements.

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones [13] "Identity-based Attacks Against Reputation-based Systems in MANETs" During this title, we are going to discuss these attacks and their countermeasures within the context of the reputation-based schemes. we are going to additionally discuss however our non-monetary, entry fee based mostly theme that's incorporated in an exceedingly name system will deter these attacks.

V. Problem Statement

The Sybil attack is very powerful, and preventing the attack has proven to be very difficult. A strategic placement of the Sybil attack can result in a significant breakdown in communication across a wireless network. In existing work in field of Sybil attack lot of research was done and it was very effective to identify the behaviour of attacker but no research was done on the analysis of attack effect in TCP and UDP protocol and also the complete information has not been provided about the network scenario like Sybil attack, behaviour etc. This was also observed in other attack studies.

VI. Proposed Security Scheme Against Sybil Attack

In this section describe the Sybil detection and protection algorithm that separated into three sections i.e. input parameters, output and routine execution. Sybil attack node behaviour stolen the id of destination in same time or different time, So that the source node not identifies the actual destination node and sends the data to the Sybil attacker node, those data are not receives by the genuine destination and all the data capture by the attacker node. Through this algorithm we efficiently detect the Sybil attacker node and protect them. Formal description of the algorithm executes step by step and guaranteed that proposed approach is more secure against the Sybil behaviour.

Algorithm: A New Attack and Prevention Scheme against Sybil Attack in Mobile Ad hoc Network

Input Parameters:

Step1: M: Mobile nodes
S_n: set of source ϵ M
D_n: set of destination ϵ M
A_1: Sybil attack different id in same time
A_2: Sybil attacker different id in different time
Routing: AODV
SDP: Sybil detector and preventer
Radio-range: 550

Output: False positive, True positive, infection percentage, PDR, Sybil node identification, NRL.

Routine:

AODV_Broadcast-rreq(S, D, AODV)

Step2: While (next-hop! = D_n && node in range) **do**
Receives packet
Incr sequence number
Forward-pkt to next-hop
Incr hop-count

Step3: Else If (D found) **then**
Established route from S_n to D_n
D_n send ack to S_n
Else
Node out of range
End if
End do
// Sybil attacker node behaviour

Step4: **If** (S_n>1 && D_n >1 && time== S_n time) **then**
A_1 in middle between S_n and D_n
If (S_n broadcast-rreq && A_1 is next-hop) **then**
A_1 send false D_{n_id} to S_n
S_n trust and send data A_1
A_1 capture and drop data from all incoming S_n
Else If (S_n>1 && D_n >1 && S_n time is not equal) **then**
A_2 send false D_n id to S_n in different time
S_n trust A_2 as D_n node & send data to A_2
A_2 capture or drop the packet
End if
End if

A. Protection:

Step5: SDP watch history profile of all neighbour
If (profile! = normal) **then**
{
Identifies packet and S_{id}, R_{id}
If (D_{id} = updated by A_{1_id} && time == S_n-time) **then**
Check packet drop or capture
Node id set A_1 categories
Else If (D_{id} = updated by A_{2_id} && time != S_n-time) **then**
Check packet drop or capture
Node id set A_2 categories
End if
End if

Step6: SDP sense the activity of all neighbour

If (next-hop receives && forward! = true && updated id of A_1== D_{n_id} && time == S_n-time) **then**

Block the A_1 node

Else If (next-hop receives && forward! = true && updated id of A_1== D_{n_id} && time != S_n-time) **then**

Block the A_2 node

End if

Re-search route from S_n to D_n

Eliminate the A_1 and A_2

Fresh route established

Send data and go to step 5 of SDP

Stop

VII. Simulation Tool Overview

The network simulator (ns-2) is a discrete network simulator targeted at network researching. Ns-2 originated in 1989 as a variant of the REAL network simulator. As a part of the Virtual Internetworks Test bed (VINT) project at the University of California in Berkley. The project was supported by Defense Advanced Research Projects Agency (DARPA) in 1995 [14]. Ns-2 is an object-oriented simulator with substantial support available for simulation of TCP, routing, and multicast protocols, initially intended for wired networks, but the Monarch Group at Carnegie Mellon University (CMU) have extended ns-2 to support wireless networks. The core of the simulator, including the network protocols is implemented in C++, while object oriented TCL is used as an interface to describe, and set up the simulations. The implementation of ns-2 closely follows the OSI model. The essential of the wireless model consist the Mobile Node at the core, with additional support for simulations of multi-hop ad-hoc network etc. A mobile node is derived from the basic Node object, with additional functionalities of a mobile wireless node, like the ability to receive and transmit signals to and from a wireless channel, and the ability to move within a given topology. In ns- 2, an agent is used as a representation of an endpoint where network traffic are constructed, processed and terminated.

Table.1 Simulation Parameters

Number of nodes	**30**
Dimension of simulated	800×800
Routing Protocol	AODV
Attack	Sybil
Simulation time (seconds)	100
Transport Layer	TCP ,UDP
Traffic type	CBR , FTP
Packet size (bytes)	512
Number of traffic	10
Maximum Speed (m/s)	Random

A. Simulation Parameter:

The simulation parameters are playing the very important role in simulation and because of that the whole network scenario is dependent. Parameters are completely decided on the basis of protocols used in simulation. The parameters are considered in this simulation are mentioned in table 1. According to these parameters the simulation of attacker and prevention scheme is simulated and measures the performance of dynamic network.

VIII. Result Analysis

In this section result analysis of normal routing , Sybil attack two scenario and IDS security against Sybil attack is evaluated. The performance of security is really provides effective after result calculation.

A. *False Detection Analysis*

The performance of network in presence of attacker is continuously degrades. The attacker aim is to drop maximum number of packets in network by communicating with multiple identities. In this graph the performance of attacker is measure according to false detection in network. False detection means the network performance is same as normal behaviour of network. It means the False Detection is always better if showing the higher percentage ratio. In this graph the false detection ratio is about only 8% maximum in Sybil 1 scenario and Sybil 2 is almost negligible. It detects the Sybil identities in network.

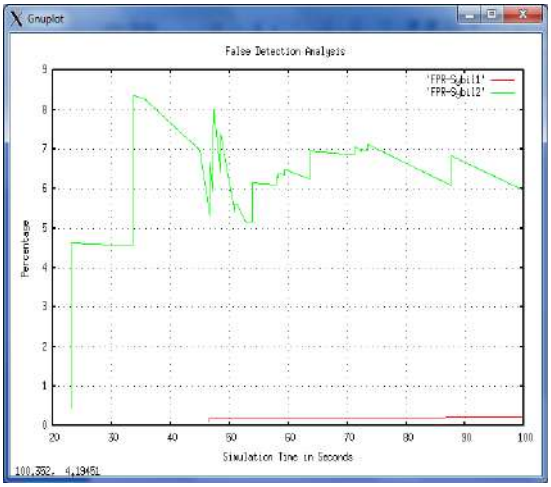

Fig.2 Attacker Infection Ratio

B. *True Detection Analysis*

The attacker detection is possible by detecting through false detection Ratio and True detection ratio in MANET. In this graph the true detection is actually shows the misbehaviour of nodes in network by that dropping of data is more. In True detection analysis the attacker existence in network is negligible or nil represents the better performance of network and also the drop percentage is negligible count in network. In this graph the attacker is positively detected and also the true detection ratio is more than 90% that shows the attacker presence in network.

C. *Infection Percenatge Analysis*

The drop percentage in presence of attacker in network is evaluated through infection percentage ratio. In this graph the Sybil attacker two modules are considered for with different Sybil identities. The drop percentage of Sybil 1scenario is minimum 30% is count, up to simulation time of 100 seconds and in Sybil scenario 2 maximum infection is 25%. But after applying security scheme th infection count is almost nil in network. The

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 02 (March - April, 2017)

proposed security scheme is enhance network performance by blocking attacker malicious activities.

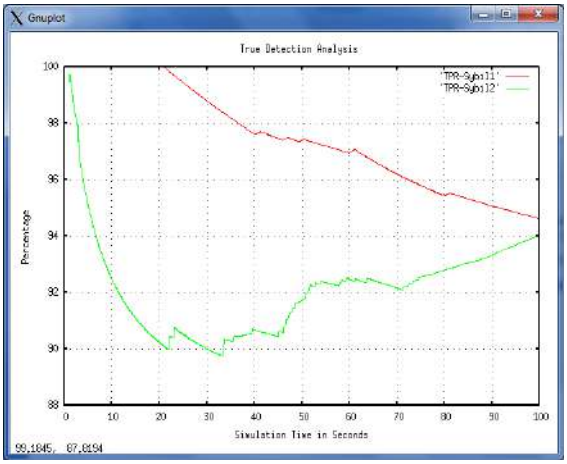

Fig.3 True Detection of Attackers

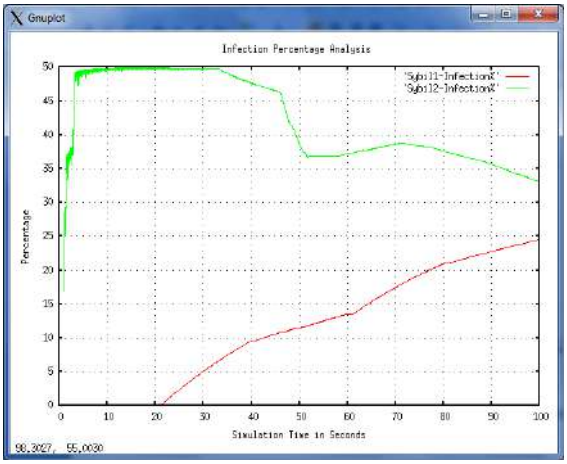

Fig.4 Attacker Infection Analysis

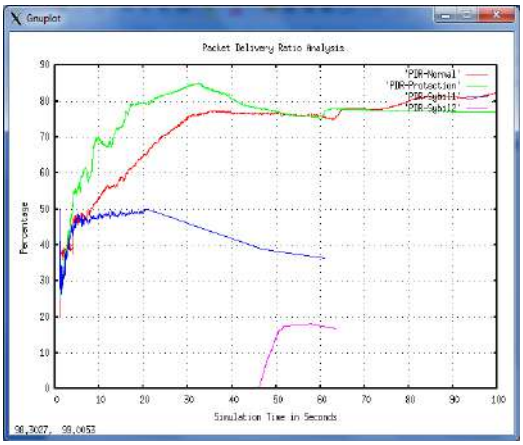

Fig.5 PDR Analysis

D. Packet Delivery Ratio Analysis

The data loss in network is reduces the packet receiving and for the reason that PDR performance is degrades. The packets percentage shows the better receiving of data with respect to sending in network. In this graph the PDR performance of normal routing, Sybil attacker presence and in presence of proposed security scheme is evaluated and the complete observation is provides the outcome in favor of proposed security scheme in MANET against Sybil attack. In this graph the PDR performance in presence of normal and protection is equal about 80% but in presence of Sybil attacker performance is very poor in dynamic network.

E. Overall Network Performance

The overall performance of network means the performance is count in network up to different scenario (like Sybil scenario-1 and Sybil Scenario-2). In this table 2 we clearly represents that the proposed security scheme is really provides the better results after blocking attacker node in network. Here the PDR, Packet Loss and other are provides the better results in network.

Table.2 Summarized Performance Analysis

Performance Metrics	Normal	Sybil1	Sybil2	Protection
SEND	3752	1051	3024	3256
RECV	3089	534	342	2505
ROUTINGPKTS	3260	205	1656	4191
PDF	82.33	50.8	11.31	76.93
NRL	1.06	0.38	4.84	1.67
Sybil Attacker Drop	0	515	2001	0
Other Reason Drop	663	2	681	751

IX. Conclusion and Future Work

The Security in MANET is the major concern of providing secure routing in between sender and receiver. The major restraint of the MANET is the limited resource capability like as bandwidth, power constraint and computational capacity. There is no centralized authority is present to monitor the networking operations. Because of that attackers are easily entered in network without any verification and permission. Misbehaviour of malicious nodes may cause damage, even fails whole of the network performance. In this paper, we proposed security against Sybil attacker misbehaviour of nodes and new approach is detected and prevent network from misbehaving nodes. The security scheme or prevention scheme is identified the attacker misbehaviour through True detection and false detection ratio in MANET. The proposed security scheme is identified the nodes having multiple identities on the basis of packet dropping in network. Routing performance of four scenarios are major first one is normal routing, second and third in presence of Sybil attack and fourth is provides security. The performance of different scenario is measured through performance metrics and the performance of proposed scheme is better. In future we propose a new algorithm for multipath routing and multicast routing in MANET. Consider the same performance metrics and identified the attacker misbehaviour through proposed security scheme in MANET. Also possible to evaluate the performance in the opinion of energy efficient routing that means evaluate the performance of routing and effect of attack in energy consumption .

REFERENCES

[1]. 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.

[2]. I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Network., Vol. 1, No. 1, pp. 13–64, 2003.

[3]. Elizabeth Belding-Royer, "Routing approaches in Mobile Ad hoc Networks", in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[4]. C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", Network Working Group Request for Comments: 3561, 2003.

[5]. Md Tanzilur Rahman, Kunal Gupta, "MANET: Security Aspects and Challenges" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6–June 2013.

[6]. Adnan Nadeem, Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials (Volume: 15, Issue: 4, Fourth Quarter 2013).

[7]. Ehsan Amiri, Hassan Keshavarz. Hossein Heidari. Author links open the author workspace, Esmaeil Mohamadi, Hossein Moradzadeh, "Intrusion Detection Systems in MANET: A Review", International Conference on Innovation, Management and Technology Research, Malaysia, 22 – 23 September, 2013.

[8]. [3]Athichart Tangpong, George Kesidis, Hung-yuan Hsu, Ali Hurson, "Robust Sybil Detection for MANETs" 978-1-4244-4581-3/09/$25.00 2009 IEEE.

[9]. Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones "Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks" 978-1-4244-9229-9/10/$26.00 2010 IEEE.

[10]. Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks" IEEE Transactions on Vehicular Technology, VOL. 59, NO. 5, JUNE 2010.

[11]. A.Rajaram. Dr. S. Palaniswami "Malicious Node Detection System for Mobile Ad hoc Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , pp. 77-85, 2010.

[12]. Md Tanzilur Rahman, Kunal Gupta,[7] "MANET: Security Aspects and Challenges" International Journal of Network Security, Vol.9, No.1, PP.22-33, July 2009.

[13]. Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones "Identity-based Attacks Against Reputation-based Systems in MANETs" ISBN: 978-1-902560-25-0 2011 PGNet.