Efficient Detection of Sybil Attack using Received Signal Strength

J. Janani
PG Scholar
Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai, India

M. Sivasankari
PG Scholar
Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai, India

***Abstract*— Mobile ad-hoc networks (MANETs) denotes complex and huge distributed systems that include wireless movable nodes that can spontaneously and dynamically self-organize into random and temporary, ad-hoc network topologies, allowing people and devices to impeccably inter network in areas with no pre-existing communication infrastructure. MANETs require a unique, different, and insistent identity per node in order for their security protocols to be feasible. This project focus on Sybil attack detection. It pose a serious threat to networks. An attack against identity in which a separate entity masquerades as many instantaneous identities is called as Sybil attack. A Sybil attacker can either create additional than one identity on a single physical device in order to launch a corresponding attack on the network or can change identities in order to weaken the detection. The major purpose is to detect Sybil nodes using received signal strength will help communication of the network be easy. The two main metrics in order to decide the detection accuracy in different environments such as true positive rate and false positive rate.**

Keywords*— Mobile Ad hoc Networks; Sybil Attack; Received Signal Strength; True positive rate.

I. INTRODUCTION

A Mobile Adhoc Network is a group of self-determining mobile nodes that can transfer data to each other nodes via radio waves. The moving nodes that are in radio range of each other can straightly communicate, whereas others need the aid of in-between nodes to way their packets. Each of the nodes has a wireless interface to interconnect with each other.

These networks are fully disseminated, and can work at any place without the aid of any static infrastructure as access points or base stations. Data traffic attack contracts either in nodes dropping data packets temporary over them or in deferring of forwarding of the data packets.

Specific types of attacks choose target packets for dropping but some of them drop all of them however of sender nodes. This may highly decrease the quality of service and increases end to end delay. Mobile Ad-Hoc Network (MANET) is basically susceptible to attack due to its major characteristics such as open standard, distributed nodes, independence of nodes participation in network (nodes can join and leave the network) and deficiency of integrated authority which can impose security on the network, distributed co-ordination and cooperation.

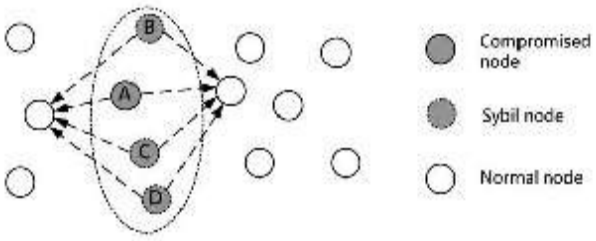

Fig.1.Sybil attack

Figure 1 shows the Sybil attack [1], the attacker disrupts the reputation system of a peer-to-peer network by generating a large number of pseudonymous characters, using them to gain an unreasonably large influence. A reputation system's susceptibility to a Sybil attack depends on how inexpensively identities can be generated, the degree to which the reputation system accepts inputs from units that do not have a chain of trust associating them to a trusted entity, and whether the repute organization gives all entities identically. An entity on a peer-to-peer system is a part of software which has right to use to local resources. An entity promotes itself on the peer-to- peer network by giving an identity. More than one identity can match to a single entity. In other words, on behalf of identities to entities is multiple to one. Entities in peer-to-peer networks must use many identities for purposes of redundancy, resource sharing, consistency and reliability. In peer-to-peer networks, the characteristic is used as a notion so that a remote entity can be awake of identities without certainly knowing the communication of identities to limited entities. By default, each different identity is typically implicit to correspond to a distinct local entity. In reality, several identities may correspond to the same local entity.

Peer-to-peer systems often trust on redundancy to diminish their necessity on potentially aggressive peers. If different identities for remote entities are not recognized either by a clear certification authority or by an unknown one these systems are susceptible to Sybil attacks, in which a small number of entities forged many identities so to compromise an inconsistent share of the system. Systems that rely upon hidden certification should be acutely mindful of this trust, since apparently unrelated changes to the relied-upon mechanism can weaken the security of the system.

A fake node or an opponent [2, 3] may present many identities to a peer-to-peer network in order to aspect and function as multiple different nodes. After becoming part of the peer-to-peer network, an attacker may then eaves-drop communications or act spitefully. By masquerading and presenting many identities, the opponent may be able to affect voting results or even significantly control the network.

II. LITERATURE SURVEY

A distributed and localized method [4] to detect system for ensuring that each physical vehicle is bound with only one identity and incorrect, vulnerable to spoof attacks. If multiple identities, claiming to be at various locations prove to be at one physical position through position verification. Traffic patterns and support from roadside base stations are used. The two weaknesses of the basic signal strength-based position verification namely, limited accuracy and Sybil witnesses. To suppress Sybil attacks in VANETs rather than eliminate individual attacks, for small-scale Sybil attacks can only make some degree of threats to VANETs. Each mobile node in the network observes packets passing through it and sporadically exchanges its interpretations in order to determine the presence of an attack. Malicious nodes making incorrect observations will be detected and rendered in effective

A hop-by-hop protocol layer between the link layer and the network layer where the abstract of each packet is signed by the sender, and the receiver or the next-hop for warder uses the signature as the proof that it has received this packet. To detect a Sybil attacker, to identify node identities that have moved on the same path. Each packet includes the location claim of the sender and the route of the receiver. The packet digest is retained using a private key of the sender. The secrecy of the private key, the sender cannot reject the packet. Upon receiving a packet, a node verifies the signature and the location of the sender. If any unreliable or invalid, it drops the packet. Otherwise, it either forwards or consumes the packet. In addition, it caches the signature of the packet and matching fields as the proof of traffic observation. Sporadically, nodes exchange these interpretations from which the path that each node has traveled can be created.

Sybil detection approach based [5] in essence on received signal strength variations. It allows a node to verify the legitimacy of nodes is composed of two balancing techniques. The first one is a localization verification method based on received signal strength. This method allows a node to verify the legitimacy of another node by estimating its upcoming geographical localizations, and compare them to its estimated localizations. When a node is detected suspicious incoherent signal strengths gradient, second technique should be used. It based on the definition of a distinguishability degree metric. This implement can be launched exclusively by every node in the network in order to detect Sybil and cruel ones based on their geographical localizations.

Spatial node distribution created by random waypoint mobility. More precisely, generalization of the model in which the pause time of the mobile nodes is chosen randomly in each way point and a fraction of nodes may remain fixed for the entire simulation time [7]. The structure of the distribution is the weighted sum of three autonomous components: the static, pause, and mobility component. This division enable to recognize how the model parameters influence the distribution. An ex-act equation of the asymptotically fixed distribution for movement on a line segment and an accurate calculation for a square area.

A reputation based scheme for MANETs that acts as a deterrent for whitewashing attacks [9]. Each node must compensation an entry fee to consume network services. As economic fees are not suitable for MANETs due to fee management problems, instead of an economic fee, use a charge in the form of cooperation. A node will receive services from the network after it collaborates until its reputation is improved to a certain level. For a normal selfish node, it is no longer valuable to perform a whitewash because it will be essential to compensation the entry fee each time it enters into the network.

Protocol similar to Needham-Schroeder to verify the identities of two nodes. A trusted base station acts as the Key Distribution Centre where all the nodes share their single symmetric key. The base station then offers a shared key for each pair of nodes to prove each other's identity. This method can limit the competence of the Sybil attack but cannot locate and remove it. If an opponent succeeds in negotiating a node, then it can create multiple fake identities to communicate with other nodes.

Robust Sybil attack [5] uses the authentication mechanism for the traffic observation. Each packet is signed by the sender private key and also signed by the nodes which are traversed by it to reach the endpoint and in the end receiver authenticate it by its public key. It gives the proof at what time and location sender transfers the packet and in which direction the packet is transfer by the sender, it will reach to the endpoint. To check the similarity of the path, it usages the novel location based Sybil attack detection mechanism. The nodes path is accurately related to each other are detected as Sybil nodes mobility can be used for the periodic change of vital security information. Direct establishment of security suggestions over the one-hop radio link resolves the well-known security-routing interdependency problem. The solution is instinctive to the users, impressionist's real-life concepts physical encounters and supports and solves some classical difficulties of security in distributed systems. In a fully self-organized and the authority-based approach stands in user contribution: In a fully self-organized approach, users need to launch security associations intentionally, whereas in the authority based method, users do not need to be aware of the founding of the security constraints, as it is done spontaneously by their node.

III. PROPOSED WORK

In telecommunications, received signal strength indicator (RSSI) is an amount of the power present in a received radio signal. RSSI is typically invisible to a user of a receiving device. However, for signal strength can vary greatly and disturb functionality in wireless networking, IEEE 802.11 devices frequently make the measurement accessible to users.

RSSI is frequently done in the intermediate frequency (IF) stage beforehand the IF amplifier. In zero-IF systems, it is completed in the baseband signal chain, before the baseband amplifier. RSSI output is frequently a DC analog level. It can also be tested by an internal ADC and the resultant codes presented directly or via peripheral or internal processor bus. There is no standardized connection of any particular physical parameter to the RSSI reading. The 802.11 standard does not describe any relationship between RSSI value and power level in milliwatts or decibels referenced to one milliwatts.

RSSI used for coarse-grained location estimations. Nevertheless, RSSI does not always available measurements that are appropriately accurate to properly determine the location. In 802.11 RSSI has been exchanged with received channel power indicator (RCPI). RCPI is an 802.11 amount of the received radio frequency power in a particular channel over the preamble and the entire received frame, and has definite absolute levels of accuracy and resolution. RCPI is entirely associated with 802.11 and as such has some accuracy and resolution required on it through IEEE 802.11k Received signal power level assessment is a necessary step in establishing a link for communication between wireless nodes. Though, a power level metric like RCPI generally cannot comment on the quality of the linkage like other metrics such as travel time measurement (time of arrival).

In an IEEE 802.11, RSSI is relative received signal strength in a wireless medium, in arbitrary units. RSSI is a sign of the power level being acknowledged by the antenna. Therefore, the higher the RSSI number, the robust the signal. RSS can be used inside in a wireless networking card to define when the volume of radio energy in the channel is under a definite threshold at which point in the grid card of the network is clear to send (CTS).

When the card is clear to send, a packet of information can be sent to the network. The end-user will expected perceive a RSSI value when calculating the signal strength of a wireless network through the usage of a wireless network perceiving tool like Wire shark, Kismet or Insider. As an example, Cisco Systems cards have RSSI Maximum value of 100 and report contains101 dissimilar power levels, the RSSI value is 0 to 100

The Sybil attacker [8] creates new uniqueness, the signal strength of that identity will be high enough to be eminent from the newly joined neighbor. In order to investigate the difference between a legitimate (true) node new comer and Sybil identity arrival behavior. Each node will seizure and store the signal strength of the communications received from its neighboring nodes. This can be achieved when a node either takes part in communicate directly with other nodes acting as a source or an endpoint or when a node does not take part in the direct communication. It will capture the signal strength values of other communicating bashes through overhearing the control frames. Each Rss-List in front of the consistent address contains Rn RSS values of recently expected frames along with their time of reaction.

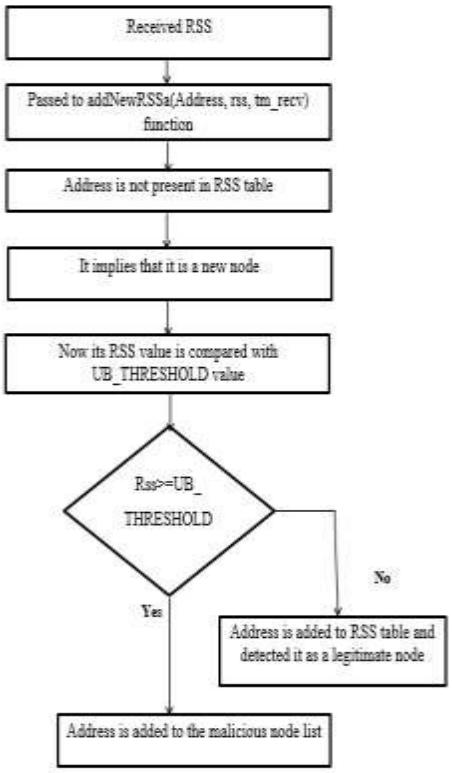

Fig.2.Overall flow graph of RSS

Figure 2 shows the normal nodes not having speed greater than 10m/s. The nodes whose speed is greater than 10m/s are identified as Sybil nodes. RSS (Received Signal Strength) upper bound threshold value is calculated and obtained. The upper bound value is considered as average of RSS value when nodes are moving at 10m/s speed. When new node enters in a network then RSS value is related with RSS upper bound value, if it is greater or equal to upper bound RSS value then it is identified as Sybil node. Three parameters in RSS are Speed, energy and frequency. Threshold value of speed is set to 10m/s but threshold value of energy is set to average energy of network and threshold value of frequency is set to average frequency of network. In this, if novel node enters a network then its Speed, Energy and frequency value must be less than threshold value then that node as legitimate node otherwise as Sybil node. When node enters in a network, firstly it is check whether its address is present in the table or not. If it is not present in the RSS table and then Speed, Energy and frequency parameters values are checked. Speed, Energy and frequency parameters values are less than threshold values then considered as legitimate node otherwise as Sybil node.

Received Signal Strength Detection method used for detecting session hijacking and capture attacks in wireless networks. The proposed scheme is created on by means of a wavelet based analysis of the received signal strength. The first improve a model to define the variations in the received signal strength of a wireless station throughout hijack, while the received signal is fixed in marked noise caused by disappearance wireless channels. An optimal filter is then considered for the purpose of detection. Using a Wavelet Transform (WT), the colored noise with composite Power Spectral Density (PSD) can be unevenly whitened. A larger Signal to Noise Ratio (SNR) higher the detection rate and decreases the false alarm rate, the SNR is maximized by investigating the signal at specific frequency ranges. The detection mechanism is validated using both network simulation and experimental results. The detector is exposed to be consistent, computationally cheap and have minimal effect on the network concert. Exposure of Sybil Nodes: No legitimate node can have speed greater than 10m/s is called as threshold value or threshold speed. In, speed, RSS value is considered and the RSS values of nodes are larger than or equal to threshold value than nodes are detected as Sybil (fake) nodes otherwise as legitimate nodes. There are two types of Sybil attacks. In the first, an attacker creates new identity while removal its previously created identity, then only one identity of the attacker is active at a time in the network. This is also called a join-and-leave or whitewashing attack and the incentive is to clean-out any bad history of mischievous activities. This attack possibly supports lack of liability in the network. In the second type of Sybil attack, an attacker parallel usages all its characteristics for an attack, called simultaneous Sybil attack.

The motivations of this attack is to cause disturbance in the network or try to improve more resources, information, access, etc. than that of a single node justifies in a network. The difference between the two is only the notion of simultaneity.

Speed based detection threshold contains two types. They are smaller speed based threshold and higher speed detection threshold. Smaller speed based threshold produce in white zones. Any new identity creation in the white zone will be detected as a whitewashing or Sybil identity because standard nodes cannot produce their first appearance in radio range. Higher speed thresholds produce wider gray zones. To infer that smaller speed based thresholds work superior than larger ones because they will produce high true positives rate. True positive rate=correctly detected whitewash ids/Total whitewash ids False positive rate=incorrectly detected good ids/Total good ids.

The nodes used by the Accuware results are capable of measuring the RSS of neighboring devices. The RSS values are measured in dBm and negative values ranging between 0 dBm (excellent signal) and -110 dBm (extremely poor signal).The RSS drops (not linearly) with the distance between the node that is receiving the signal and the device that is communicating the signal. The RSS detected by the nodes are affected by numerous factors, including:

- The antenna of the device that is transmitting.
- The antenna of the node itself.
- The number of walls and other obstructions in closeness of the nodes.
- The material of the substances inside the environment.

The Sybil attacker creates new uniqueness, the signal strength of that identity will be high enough to be eminent from the newly joined neighbor. In order to investigate the difference between a legitimate (true) node newcomer and Sybil identity arrival behavior.

Each node will seizure and store the signal strength of the communications received from its neighboring nodes. This can be achieved when a node either takes part in the communicate directly with other nodes acting as a source or an endpoint or when a node does not take part in the direct communication. It will capture the signal strength values of other communicating bashes through overhearing the control frames. Each RSS-List in front of the consistent address contains Rn RSS values of recently expected frames along with their time of reaction.

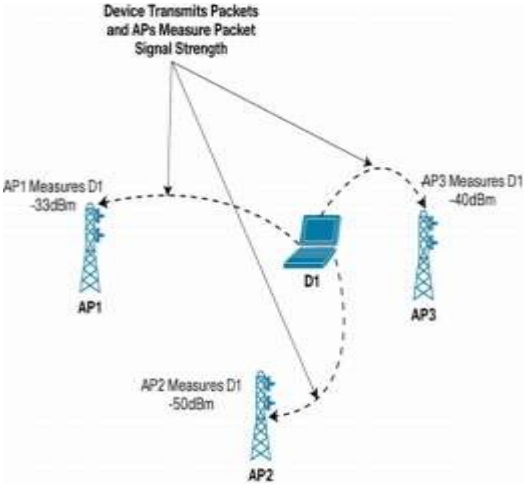

Fig.3. Received Signal Strength

A. Received Signal Strength Detection method

To detect session hijacking and capture attacks in wireless networks. Figure 3 shows the RSS can created on by means of a wavelet based analysis of the received signal strength. The first improve a model to define the variations in the received signal strength of a wireless station throughout hijack, while the received signal is fixed in marked noise caused by disappearance wireless channels. An optimal filter is then considered for the purpose of detection. Using a Wavelet Transform (WT), the colored noise with composite Power Spectral Density (PSD) can be unevenly whitened. A larger Signal to Noise Ratio (SNR) higher the detection rate and decreases the false alarm rate, the SNR is maximized by investigating the signal at specific frequency ranges. The detection mechanism is validated using both network simulation and experimental results. The detector is exposed to be consistent, computationally cheap and have minimal effect on the network concert. Exposure of Sybil Nodes: No legitimate node can have speed greater than 10m/s is called as threshold value or threshold speed. In, speed, RSS value is considered and the RSS values of nodes are larger than or equal to threshold value than nodes are detected as Sybil (fake) nodes otherwise as legitimate nodes.

There are two types of Sybil attacks. In the first, an attacker creates new identity while removal it's previously created identity, then only one identity of the attacker is active at a time in the network. This is also called a join-and-leave or whitewashing attack and the incentive is to clean-out any bad history of mischievous activities. This attack possibly supports lack of liability in the network. In the second type of Sybil attack, an attacker parallel usages all its characteristics for an attack, called simultaneous Sybil attack.

The motivations of this attack is to cause disturbance in the network or try to improve more resources, information, access, etc. than that of a single node justifies in a network. The difference between the two is only the notion of simultaneity.

Speed based detection threshold contains two types. They are smaller speed based threshold and higher speed detection threshold. Smaller speed based threshold produce in white zones. Any new identity creation in the white zone will be detected as a whitewashing or Sybil identity because standard nodes cannot produce their first appearance in radio range. Higher speed thresholds produce wider gray zones. To infer that smaller speed based thresholds will work better than larger ones because they will produce high true positives rate. True positive rate=correctly detected whitewash ids/Total whitewash ids False positive rate=incorrectly detected good ids/Total good ids.

IV. SYSTEM IMPLEMENTATION

To analyze the performance metrics in Network Simulator (NS2.35) of various true positive rate and false positive rate with different kinds of speed and density in the networks. The UB−THRESHOLD be around RSS value (in Watts) of some scenarios when a transmitter is stirring with 10 m/s speed; lower speeds thresholds will increase detection accuracy. The TIME−THRESHOLD is the typical (maximum) time in which a node should listen from another node, otherwise that identity will be measured as out of range or previous identity of a whitewasher. Shorter time intervals will rise identity revalidations in the network; while lengthy intervals will increase table sizes in network nodes. The LIST−SIZE is the maximum RSS records reserved for an identity or address.

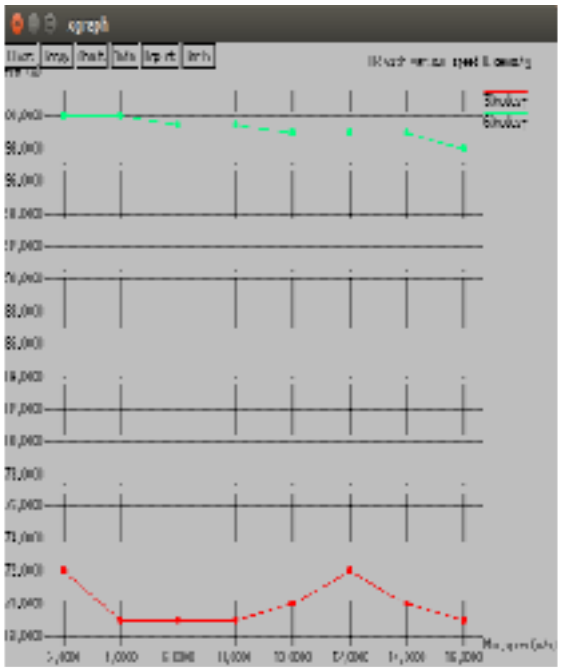

Fig.4. True Positive Rate

Figure 4 shows the true positive rate and maximum speed of the networks is high in nodes 60 and the true positive rate is less in nodes 30

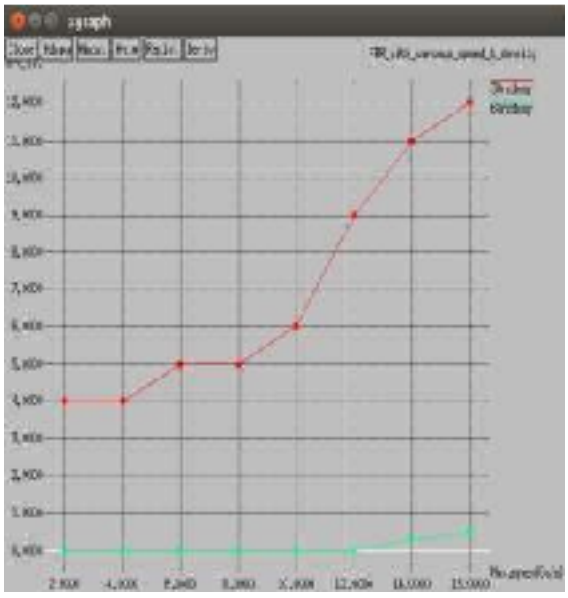

Fig.5. False Positive Rate

Figure 5 shows the false positive rate and maximum speed of the networks is low in nodes 60 and the false positive rate is high in nodes 30

V.CONCLUSION

Sybil attack detection showed high true positive rate in terms of speed, energy and frequency. But compared to the Robust Sybil attack detection method, the accuracy was low; due to nodes is travel in single path. But the RSS detection method was higher than Robust Sybil attack detection incurred many whitewash attack (fake) identities are disturbing the communication in the network. RSS showed better overall accuracy in terms of speed, distance, energy and frequency. Sybil attack detection is the main intelligent part in the Mobile Adhoc- Networks. In order to detect Sybil attacks in many detection methods, the accuracy rate of true positive rate is 90%. In future, to detect and deploy new mitigation technique to eliminate Sybil attack and communication of the network is easy to improve accuracy in MANETs.

ACKNOWLEDGMENT

We are very much thankful to Mr.S.Prasanna, Assistant Professor of Computer Science and Engineering department for his valuable guidance, encouragement, co-operation and timely help to complete this work.

REFERENCES

[1] J. Newsome, E. Shi, "The Sybil Attack in Sensor Network: Analysis & Defenses," The Third International Symposium on (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.

[2] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack," Univ. Mass. Amherst, Amherst, Tech. Rep. 2006-052, 2006.

[3] J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[4] B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil nodes in VANETs," presented at the Proc. 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, 2006, pp. 1–8.

[5] A. Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, "Robust Sybil detection for MANETs," in *Proc. 18th ICCCN* 2009, pp. 1–6.

[6] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," *Int. J. Netw. Security*, vol. 8, pp. 322–333, May 2009.

[7] Gilles Guette, Reeta Mishra, (2012), "Quantifying Resistance to the Sybil Attack" - VSRD International Journal of Computer Science and Information Technology, Vol.2, No. 11, pp. 890-894.

[8] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones," Lightweight Sybil Attack Detection in MANETs", IEEE Systems Journal, Vol. 7, No. 2, June 2013

[9] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks," in *Proc. WD IFIP*, 2010, pp.1–6.

[10] H. Liming, L. Xiehua, Y. Shutang, and L. Songnian, "Fast authentication public key infrastructure for mobile ad hoc networks based on trusted computing," in *Proc. Int. Conf. WiCOM*, 2006, pp. 1–4.

[11] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 3, pp. 257–269, Jul.–Sep. 2003.

[12] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," in *Proc. 3rd WRAITS*, 2009, pp. 21–26.

[13] Shuiyu, Wanlei zbou, Weijia jia, Song Guo, Yong Xia and Feilong Tang, (2012), "Detection and Localization of Sybil Nodes in VANETs" - IEEE transactions on Mobile Computing, Vol.23, No.6, pp. 1073-1080.