Australian Journal of Basic and Applied Sciences, 9(33) October 2015, Pages: 443-453

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Detection And Prevention Of Sybil Nodes Using Threshold And Security Based Techniques In Manets.

[1]N.Geetha and [2] DR.P. Sivakumar

[1]M. Tech Student, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.
[2]Professor, Department of Information Technology, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.

ARTICLE INFO

Article history:
Received 10 September 2015
Accepted 15 October 2015
Available online 24 October 2015

Keywords:
MANET, Sybil, Signal Strength, Centralized Validation

ABSTRACT

The Mobile ad hoc Networks (MANETS) are considered to be a complex distributed system which can organize itself or self configured. Due to its complex nature, MANETS suffer from different security issues which needs the solution to be defined. One among the attack is Sybil, on which the identity of the nodes are duplicated. MANETS need a unique, distinct identity for each node in order to perform its operations. Sybil attack is considered to be a severe high end threat to the network. Under Sybil Attack, an attacker tries to create multiple identity for a single node in other terms(a physical device). Hence in order to spot and cover the Sybil node, the concept of Received Signal Strength and Trusted Keying Mechanism. To prevent the Sybil node, a new concept called centralized validation technique is used. It is proven to be more efficient than the existing technique.

To Cite This Article: N.Geetha and Dr. P. Sivakumar., Detection And Prevention of Sybil Nodes Using Threshold And Security Based Techniques In Manets., ***Aust. J. Basic & Appl. Sci.,*** *9(33): 443-453, 2015*

INTRODUCTION

MANET is generally considered as the infrastructure less network and self-configuring nature. The devices connected to the MANET are allowed to move freely across the network as it deals with the wireless medium. As the nodes move in a random direction or path, the links among the nodes changes frequently. Each node, which is moving from its path, should be forwarding the traffic, which carries the packets to the other nodes. On the other terms, the forwarding node acts as the routing node. The main primary challenging aspect of MANET is considered to be the maintenance of node information periodically and route the traffic accordingly. A MANET is capable of operating itself and or it can be connected to the larger Internet. It consists of a routable networking environment on top of a Link_Layer_ad hoc network.

MANET has become the key area of research because on the last recent years for many researchers because of the challenges it possess to the related protocols. In this paper, a technique to detect and prevent the MANET from SYBIL attack is defined. A SYBIL is generally defined as one kind of vulnerability threat that is imposed on a wireless network to affect the network performance. As the MANET enables users to communicate without any physical infrastructure regardless of their geographical location, the SYBIL attack is easily injected on the network. The nodes in the MANET are self-organizing and adaptive. Hence a Node or Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.

As the nodes in MANET are continuously in motion, the message or data routing is a key problem in a decentralized environment where the topology keeps on fluctuates. Since the shortest path from the source to destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the

Corresponding Author: N.Geetha, M.Tech Student, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Pondicherry University, Pondicherry, India.
E-mail:geethakodis12@gmail.com

ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack, Sybil attack etc. SYBIL attack degrades the performance of the network by creating multiple identities of a single node. The SYBIL node is injected to the network and it travels along the other nodes as the topology changes. This paper discusses about the various techniques involved in detecting and preventing the Sybil Attack. SYBIL attack detection using RSS (Received Signal Strength) is implemented in this paper.

II Related Work:

A. Resource Testing Method:

Resource Testing is considered to be the most frequent and common technique involved in preventing the SYBIL attacks. The significant step involved in this is that the quantum of computing resources of each entity on the network is limited. In this method, the various tasks are widely distributed to all identities of the network in order to test the resources of each node and to determine whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity.

Main contribution of this method is considered to be analyzing each identity for many resources. In case of any discrepancies, the compromised node will be identified and spotted down. The resource in this method initially indicates the storage computation and communication. But when the system like WSN is concerned, an attacker may have storage and computation resources in large capacities compared to resource-starved sensor nodes. On the other side, if identity is done based on messages via verification, it might flood the entire system itself. So Finally all the above choice are inadequate for wireless sensor networks.

Limitations:

Two major things are considered in this approach as less efficient or disadvantage, That is, in several applications very little Sybil identities are needed to launch an efficient Sybil attack. And on the other side, the intruder can get hold of network resources like storage, network card, memory etc to complete malicious tasks.

B. Recurring Costs and Fees technique:

This approach is considered bit far better than the previous one, here the identities are periodically re-validated in the network. It is considered to be a costlier approach when compared to Resource testing method. Here in this method the each participating identity is periodically or one-time charged with a fee. Recurring costs and Fees Technique differs from resource testing where resource tests are conducted after specific time intervals to impose a certain "cost" on the attacker that is incurred for every identity that he controls or introduces into the network. However a number of researchers that have endorsed this method have used computational power in their resource tests.

The Recurring fee per identity which are participating is proposed by Margolin *et al* where recurring fee per participating identity is imposed in order to deter Sybil attackers. Out of this, there is another way of approach where the fee is applied on the resources and it is considered to be deterrent than a Recurring Cost. Here the recurring fee is considered not a payment process, but as the non-payment security mechanism such as CAPTCHAs, charged SMS messages, or cooperation in the network. But though after applying all these techniques, the attacks are still not controlled and the security mechanisms are in adequate. The malicious user spends or incurs only one-time cost (for computing resources) that may be recovered via the execution of the attack itself, as pointed out by Levine *et al*. It is concluded that the recurring costs or fees per identity is more effective as a deterrent to Sybil attacks than a one-time resource test.

Limitations:

For many applications, recurring fees can incur a cost to the Sybil attack that increases linearly with the total number of identities participating; one-time fees incur only a constant cost.

1) C. Trusted Devices Method:

In this method, the devices are linked to a specific fashion to a specific hardware device. This is a one-to-one mapping of a hardware device and a network entity. Here any hardware device that may be a network card or router is bounded to the single network entity. But though, there is no solution met to prevent the entity from obtaining more than one hardware devices. This process could be explained with a scenario, where an attacker tries to install two network cards using only one hardware. Here in this case, the attacker tries to create multiple identities. It is considered to be analogous to any central authority handing out cryptographic certificates. And moreover there are no special methods of preventing an attacker from obtaining multiple devices other than manual intervention. The cost of acquiring multiple devices may be high, however.

2) This idea is proposed from the concept of already existing method, which is called as Trusted Certification, where the central node issues the certificates to the neighbor nodes. So based on that idea, some research suggested the usage of trusted devices or trusted modules that store certificates, keys, or authentication strings previously assigned to users by a centralized authority. Such devices are hard to obtain because of their potentially high price, and hence can be used to limit opportunities for Sybil attacks. Examples of such mechanisms are proposed by Rodrigues *et al*. and Newsome *et al*. , although the latter work is on wireless sensor networks. In theory, when the intent of the attacker is known in advance, these defenses might be effective. However, in cases such as anonymity (Tor, for instance) and recommender systems, given that fewer Sybil identities can cause great harm, these defenses are obsolete.

Limitations:

The cost of acquiring multiple devices may be high, however.

3) D. Mutual Agreement:

Users can activate a point-to point secure side channel (SSC) using infrared or wired media between their personal devices to authenticate each other and set up shared keys when they are in close proximity to each other. The author attempts to solve the problem of impersonation and Sybil attacks by binding a user's face and identity using these SSCs. However, SSCs are based on the assumption that nodes are connected through wired or infrared connections.

In this method, the authors have shown that mobility can help to provide security in mobile networks. They illustrated the approach on two application scenarios in the area of mobile ad hoc networks: networks with an offline authority and fully self-organized networks. In the first scenario, a direct establishment of security associations over the (one-hop) radio link solves the well-known security-routing interdependency problem. In the second scenario, the authors have shown that the solution is intuitive to the users, as it mimics real-life concepts (physical encounters and friends) and solves some classical problems of security in distributed systems. The techniques works both with public-key and with symmetric cryptography and the related protocols are provided.

The authors have studied the pace of establishment of the security associations under various mobility scenarios. In particular, they have extended the Random Waypoint model by introducing the concept of meeting points in order to be closer to human behavior. They have shown that in self-organized scenarios, the set-up of security associations can take several hours, while in the case of networks controlled by central authorities, this time can be as low as 20 minutes. It has also been further shown that the vast majority of the security associations are set up in much shorter time than the full set of security associations. This is an important observation, that secure routing is also possible in networks in which only 40 percent of security associations are established. Moreover, if the users are willing to set up security.

E. PASID Method:

It is proposed to detect Sybil identities by observing node dynamics. Nodes are keeping track of identities which are often seen together (Sybil identities) as opposed to the honest distinct nodes that move freely in different directions. However, the scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target.

In this paper, the authors show that the mobility of nodes in a wireless network can be used to detect and identify nodes that are part of a Sybil attack. They rely on the fact that while individual nodes are free to move independently, all identities of a single Sybil attacker are bound to a single physical node and must move together. Piro et. al. proposed two initial methods, both passive, that can be run on standard, inexpensive equipment without any special antennae or hardware and with only very loose clock synchronization. In the first method, called Passive Ad hoc Sybil Identity Detection (PASID), a single node can detect Sybil attacks by recording the identities, namely the MAC or IP addresses of other nodes it hears transmitting. Over time, the node builds a profile of which nodes are heard together, which helps reveal Sybil attackers. The simulation results shows that in networks with sufficient connectivity and mobility PASID can produce close to 100% accuracy in identifying the various attacker identities while avoiding any false positives. As the network becomes more dense, with more nodes in less space, the false positive rate increases; as it becomes more sparse, the accuracy rate declines as each node has fewer chances to hear its neighbors. To combat this, the multiple trusted nodes can share their observations to increase the accuracy of detection over a shorter time or in a more-sparsely connected network.

The second method, PASID with Group Detection (PASID-GD), extends the approach and reduces false positives that can occur when a group of nodes moving together is falsely identified as a single Sybil attacker. By monitoring collisions at the MAC level these cases can be differentiated. This approach is successful because an attacker operating over a single channel can transmit only serially, whereas independent nodes can transmit in parallel, creating detectably higher collision rates.

Drawbacks:

This scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target.

F. BARTER Method:

This method is a behavior-based access and admission control system for MANETs in which nodes initially exchange their behavior profiles and calculate individual local definitions of normal network behavior. During admission, each node issues an individual decision based on its definition of normalcy. These individual decisions are then combined via a threshold cryptography that requires agreement among a fixed amount of MANET nodes to change the status of the network.

BARTER is an adaptation of BB-NAC for fully distributed networks. As in the BB-NAC mechanism , a newcomer would present its behavior profile to the MANET members during admission control. If an agreement is reached among the members, the newcomer is admitted into the MANET. Analogously, during access control, the traffic exchanged would be checked against the behavior profiles of similar MANET members to perform anomaly detection. Unlike BB-NAC, the admission and access control decisions in BARTER are distributed among the MANET members rather than being centrally performed by a NAC enforcer. The decision of each individual MANET member is based on the accumulation of knowledge gathered from the behavior profiles of other members. Ultimately, the final admission or access control decision is achieved by building BARTER on top of a threshold cryptographic infrastructure that guarantees not only distributed decision making but also secure communications among MANET members. Due to the limited computational resources of many MANET platforms (such as cell phones or PDAs), the calculation of *clusters of behavior profiles* similar to the one implemented in the BB-NAC mechanism would not be feasible. Instead, BARTER takes advantage of the restrictions imposed by the threshold cryptographic infrastructure as a way to approximate groups of similar behavior within the network.

The main contributions of the BARTER mechanism are the following: – A mechanism that provides automatic and fully distributed creation of admission and access policies for MANETs. Individual decisions are made by each MANET member based on the knowledge accumulated from previous profile exchanges among members. The final admission or access control decision is determined from the aggregation of individual decisions using a threshold cryptographic layer that runs under the BARTER mechanism. BARTER 195 – A mechanism that is robust against attacks from MANET members. The mechanism adjusts over time in order to maintain its robustness even in the presence of malicious devices within the MANET. – An extensive evaluation of the mechanism using hundreds of content and volumetric behavior profiles computed from the ENRON dataset.

Drawbacks:

This method is not so efficient in tracing the behavioral characteristics of a host using techniques such as bagging or boosting.

III. Existing System:

Sybil attacks are a fundamental threat to the security of distributed systems. Recently, there has been a growing interest in leveraging social networks to mitigate Sybil attacks. However, the existing approaches suffer from one or more drawbacks, including bootstrapping from either only known benign or known Sybil nodes, failing to tolerate noise in their prior knowledge about known benign or Sybil nodes, and not being scalable. In this paper, the authors has proposed a mechanism to overcome these drawbacks. Toward this goal, they introduced Sybil Belief, a semi-supervised learning framework, to detect Sybil nodes. Sybil Belief takes a social network of the nodes in the system, a small set of known benign nodes, and, optionally, a small set of known Sybils as input. Then, Sybil Belief propagates the label information from the known benign and/or Sybil nodes to the remaining nodes in the system. The Sybil Belief is evaluated using both synthetic and real-world social network topologies. It has been shown that the Sybil Belief is able to accurately identify Sybil nodes with low false positive rates and low false negative rates.

Sybil Attack:

Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority to verify these identities. An attacker can exploit this property and send control packets, for example RREQ or RREP, using different identities; this is known as a Sybil attack. A Sybil attack is essentially an impersonation attack, in which a malicious device illegitimately fabricates multiple identities, behaving as if it were a larger number of nodes (instead of just one). This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other severe attack.

The Sybil attack in P2P networks first mentioned by Douceur (2002) shows that, if a single malicious entity can present multiple identities this entity can control the whole network. He argues that under realistic assumptions of resource distribution and coordination only a central organized authority can prevent from a Sybil attack. But he says that implicit identification authorities like ICANN can be sufficient for Sybil resistance if they are mindfully used.

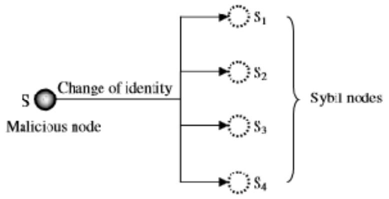


Fig. 1: A Sybil Attack with multiple identities.

IV. Proposed System:

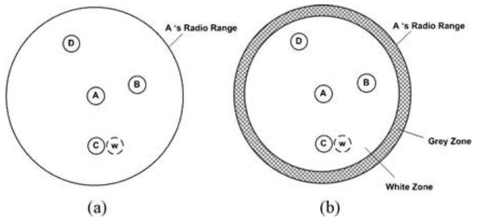


Fig. 2: Range of coverage

Since MANETs require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network. In this project, we propose two techniques for the efficient detection of Sybil nodes known as the RSS and the Trusted key techniques. Also a prevention mechanism called the Centralized Validation Technique is proposed for preventing the Sybil attacks in MANET.

The proposed system comprises of two main things namely.

1. Detection of Sybil Nodes.
2. Prevention of Sybil Attack.

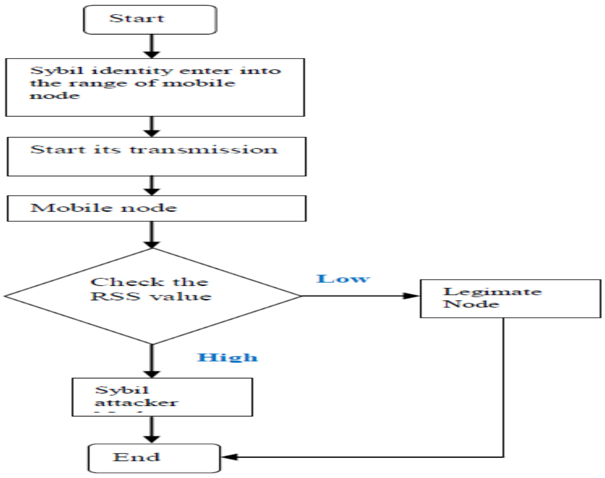


Fig. 1: Flow diagram.

Detection of Sybil Nodes:

We introduce two techniques for the detection of Sybil nodes in MANET. The two techniques are listed below

1. Received Signal Strength method (RSS).
2. Trusted Key method (TK).

Received Signal Strength Method (RSS):

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. For example, new legitimate nodes become neighbors as soon as they enter inside the radio range of other nodes; hence their first RSS at the receiver node will be low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood. When the Sybil attacker creates new identity the signal strength of that identity will be high enough to be distinguished from the newly joined neighbor.

Detection:

We will setup our detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighborhood.

Algorithm:

```
addNewRss (Address, rss, time−recv)
BEGIN SUB:
IF: Address is not in the Table
THEN:
IF: rss >= UB−THRESHOLD
THEN: Add−to−Malicious−list(Address)
Bcast−Detection−Update(Address)
ELSE: Add−to−Table(Address)
END−IF
Create−Record(Address)
Push−back(rss,time−recv)
IF: list−Size > LIST−SIZE
THEN: Pop−front()
END SUB:
```

Algorithm 2

```
IF: RSS−TIMEOUT
THEN: rssTableCheck( )
rssTableCheck( )
BEGIN SUB:
FOR: for each Address in the Table
DO:
Pop−element()
IF: (Current−Time—getTime()) > TIME−THRESHOLD
//Indicating that we did not hear from this Address since the TIME−THRESHOLD
THEN:
IF: getRss() > UB−THRESHOLD
THEN: Add−to−Malicious−List (Address)
//Indicates previous ID of a Whitewasher
ELSE: Print “Normal out of Range”
END FOR:
END SUB:
```

V. Architecture Diagram:

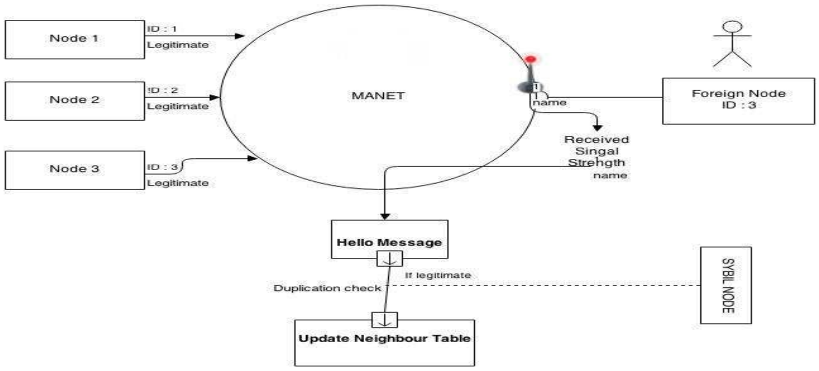


Fig. 3: Architecture of RSS Module

Trusted Key Method:

The keying mechanism is used in order to transfer the broadcast message from one node to the other. Upon doing this the nodes shares the common key. Using this method we spot down the Sybil Node. That is, once a node shares the key for broadcasting, then the same node cannot reuse the key. In this case, when the multiple entries exist for a single node, then the Sybil Node could be spotted down.

Steps involved:

Step: 1. The malicious node xm will have to generate a Sybil node such that its ID is minimum in the network, henceforth it is found by a trusted key method, i.e., if xs is a Sybil node’s identity then
xs < xi

Step 2. In the next step, all nodes will have their own individual key, in this case all transmission of packets will be done only by sharing the trusted key. The malicious node xm will introduce itself and its Sybil node to the network. To achieve this, the malicious node broadcasts the Hello packet with its original ID. Let n neighboring nodes respond with their respective IDs but with the same key.

3. The key once used cannot be reused by any other node. Hence all nodes share their own key to establish the connection with the neighbor node…Next time the malicious node will use its Sybil node to broadcast the Hello packet, by decreasing its transmission power. This variation in the transmission power is required to convince other nodes in the neighborhood that it is not the same malicious node. Otherwise, a Sybil attack can be detected on the basis of the following facts:

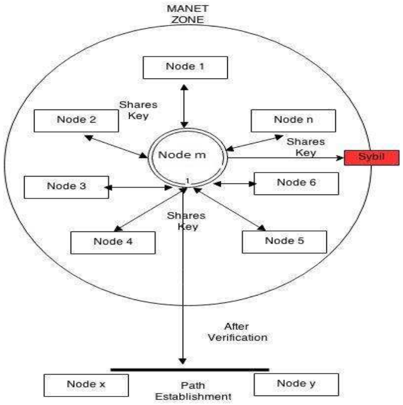


Fig. 4: Architecture of Trusted Keying Module.

a. Sybil nodes of a malicious node will always move together.
b. Two different physical entities in the MANET cannot have the same set of the neighbors.
c. The received signal strengths of the messages sent by the attacker node and its Sybil nodes will be almost the same (there can be some variation due to the movement of nodes).
4. In this manner, the Sybil nodes can be detected by trust key the number of nodes that will respond to the Sybil Node will always be less than or equal to n; i.e. if n’ is the number of nodes that responded to the Sybil node then n’ <= n.
5. During the election process, every node will broadcast its neighbor list, including itself. Since the ID of the Sybil node is the smallest in the whole network, it will always defeat the lowest ID clustering scheme by becoming the cluster head again and again

Preventing The Sybil Attack:

Centralized Validation Technique:

Sybil attacks can be avoided by using trusted certification. This type of method assumes that there is a special trusted third party or central authority, who can verify the validity of each participant, and further issues a certification for the honest one. In reality, such certification can be a special hardware device or a digital number.

Note that essentially both of them are a series of digits, but are stored on different medias. Before a participant joins a peer-to-peer system, provides votes, or obtains services from the system, his identity must first be verified. Actually, this method is the most commonly used Sybil defense in our daily lives. For example, when we are applying for a credit card, we need to provide our social security number for verification; when we are voting in election years, we also need our official ID card for getting a ballot. When a malicious user launches Sybil attacks, defense mechanisms usually require that a message be sent together with a signature, which could be used for authenticating the validity of the sender or the data. Actually, according to a paper, trusted certification is the only approach that has the potential to completely eliminate Sybil attacks. Since almost all authentication steps require the participation of the central server, we categorize this type of solution as a centralized trusted certification.

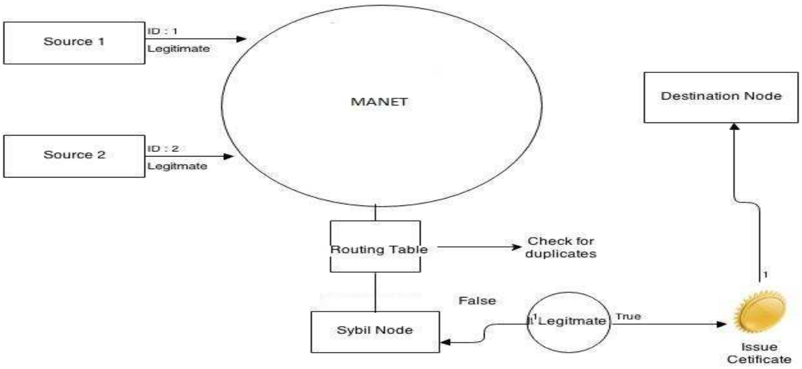


Fig. 5: Architecture of Centralized Validation.

Steps Involved:

Step 1 : Select edges with high local betweeness as suspicious edges.

Step 2 : Use signed certificate network-based Sybil detection mechanism to determine honest and Sybil.

Step 3: Find shortest paths from the honest nodes to Sybil nodes.
Step 4: Compute the visiting frequency of edges.
Step 5: Take the edges with high visiting frequency as suspicious.
Step 6: Certificate Verification:
Step 7: Generate the initial neighbor set, {u}, {v}, and {w}.
Step 8: Compute the number of unique paths from {v} to {u}, and from {v} to {w}
Step 9: for Predefined times do
Step 10: Respectively add _k disjoint neighbors into {u}, {v}, {w}.
Step 11: Compute the number of unique paths from {v} to {u}, and from {v} to {w}
Step 12: Compute the growing speeds of unique paths.
Step 13: if it is greater than a threshold then
Step 14: Attack Edge Detection:
Step 15: Find attack edges from detected nodes by distrust relations; break them.

VI . Simulation Model And Parameters:

Table 1: Simulation Parameters.

Parameter	Value
Area	1000m x 1000m
Speed	2 to 10 m/s
Pause Time	10 s
Radio Propagation Model	Two - ray ground reflection
Radio Range	250m
Carrier Sense Range	550m
Number of Nodes	20
MAC	802.11
Application	CBR, 10 to 40
Packet Size	64 B
Simulation Time	600 s
Movement	Random Waypoint Model
Placement	Uniform

The experiment uses NetworkSimulator-2 and version is NS2.33. Our simulated network consists of 20 mobile nodes placed randomly within a 1000 m x 1000 m area. Each node has a transmission speed of 10Mbps.The mobility model chosen for a mobile node was the two-ray ground model and traffic type is constant bit rate (CBR). The MAC type is IEEE 802.11 MAC Layer is used and the packet size is 64 bytes, the omnidirectional antenna is used for this work. Table 5.1 lists the values of the common parameters used in all the experiments.

A. Performance Metrics:

i. Packet Delivery Ratio:

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources, it can be termed as:

$$\text{PDR} = \frac{\sum \text{Number of data packets received}}{\sum \text{Number of data packets sent}}$$

ii. Average End-to-End Delay:

The average end to end delay is the average time it takes for a data packet to reach the destination. These consist of all probable delays caused by buffering through route discovery, latency, queuing at the interface queue. This metric is considered by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination, it can be defined as:
Avg. End to End Delay = S/N

Where S is the sum of the time taken to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

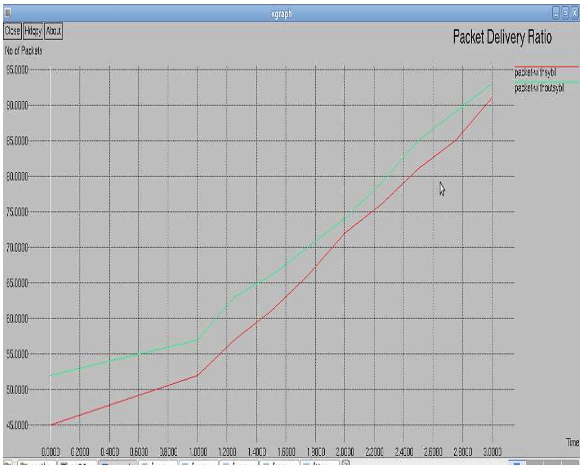
B. Simulation Experiment:

According to the experimental point of view, the RSS of nodes are evidence in order to determine the behavior of the new legitimate nodes and the Sybil attacker's new identities. The detection threshold is setup based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from beginner, if greater than the threshold imply irregular entry into the neighborhood. 10 m/s is worned as an upper bound speed because it is believed that in most of the ad hoc network applications including vehicular ad hoc networks in urban or congested areas, nodes usually may not move faster than 10 m/s (36 km/h) hence this speed is selected to be a good upper limit for the proposed technique. The performance of the various metrics like packet delivery ratio, throughput and average end to end delay are calculated.

RESULT AND DISCUSSION

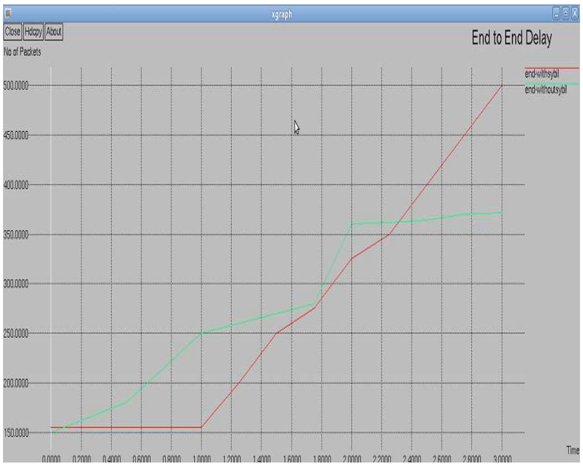
The comparison graph shows the results for the three techniques with a better performance when the Sybil nodes are prevented. The performance metrics like Packet Delivery Ratio and End to End Delay are studied for the proposed three techniques.

- ***RSS Technique:***
  Packet Delivery Ratio:



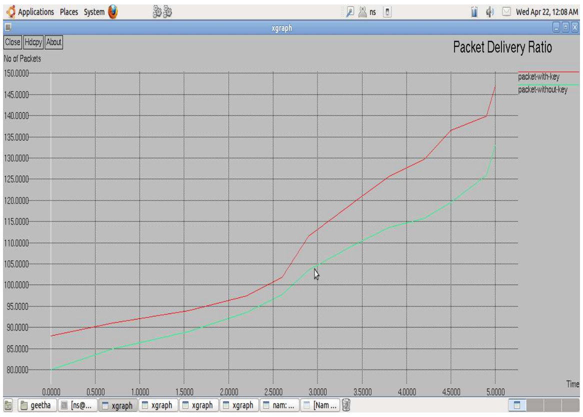
From the above graph, using the RSS Technique, the packet delivery ratio is efficient by 5% without the presence of the Sybil nodes.

- ***End to End Delay:***



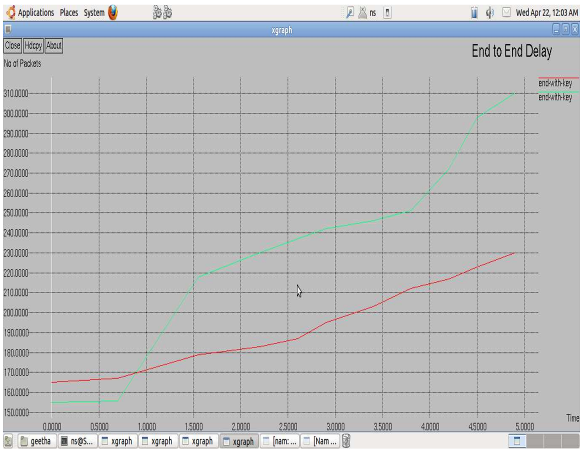
The End to End Delay of the proposed work is decreased by 4% without the presence of the Sybil node.

- ***Trusted Key Technique:***
- ***Packet Delivery Ratio:***



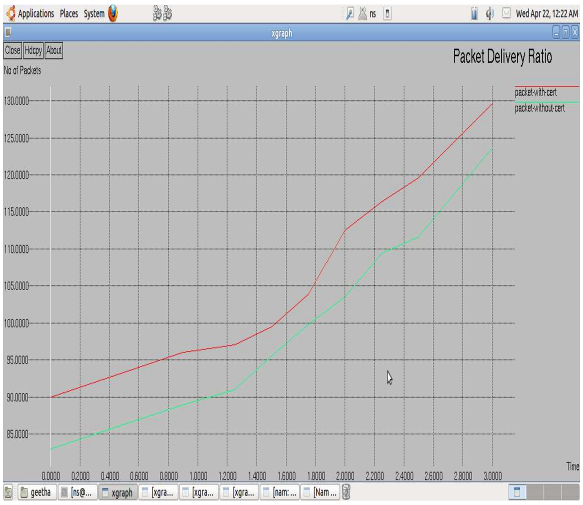
The packet delivery ratio of the proposed work is 8% efficient with the presence of the Sybil node.

- ***End to End Delay:***



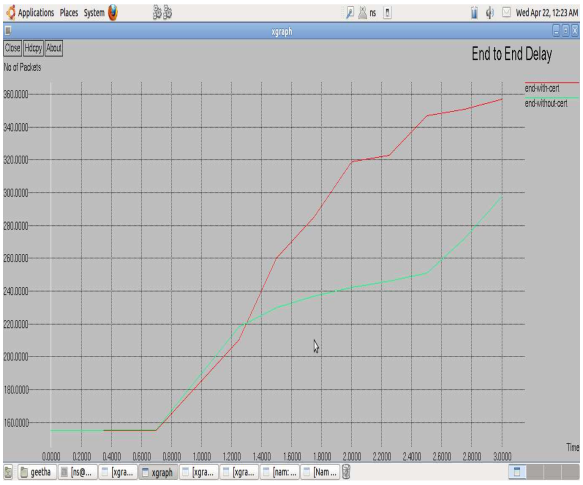
The End to End delay of the proposed work is 6% efficient than the presence of Sybil nodes.

- ***Centralized Validation Technique:***
- ***Packet Delivery Ratio:***



The packet delivery ratio of the proposed work is 10% efficient without the presence of the Sybil node.

- ***End to End Delay:***



The end to end delay of the proposed work is 8% efficient than the presence of the Sybil node.

VIII. Conclusion:

MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe communication it is must be a secured network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, it uses multiple identities or uses the identity of another node present in the network to disrupt the communication or reduce the trust of legitimate nodes in the network. In this project a new technique, the RSS based detection approach along with the authentication of node called the Trusted key which will correctly identify the Sybil identity is proposed. Authentication of node allows only legitimate node to come in to the network. As well as a Centralized Validation Technique is proposed to prevent the Sybil attack in the mobile ad hoc network. As a future enhancement these techniques can be adopted to identify other types of attacks such as denial of service attack, rushing attack and so on.

REFERENCES

Chlamtac, I., M. Conti, J.J.N. Liu, 2003. Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Netw., 1(1): 13–64.

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

Newsome, E., D. Shi, Song, A. Perrig, 2004. "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 259–268.

Parno, B. and A. Perrig, 2005. "Challenges in securing vehicular networks," in Proc. 4th Workshop HotNets, 1–6.

Hoeper, K. and G. Gong, 2007. "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in Security in Distributed and Networking Systems (Computer and Network Security). Singapore: World Scientific.

Hashmi, S. and J. Brooke, 2010. "Toward Sybil resistant authentication in mobile ad hoc networks," in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 17–24.

Chen, Y., J. Yang, W. Trappe, R.P. Martin, 2010 "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Veh. Technol., 59(5): 2418–2434.

Bouassida, M.S., G. Guette, M. Shawky, B. Ducourthial, 2009. "Sybil nodes detection based on received signal strength variations within VANET," Int. J. Netw. Security, 8: 322–333.

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

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

Suen, T. and A. Yasinsac, 2005. "Ad hoc network security: Peer identification and authentication using signal properties," presented at the Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW), New York, Jun., pp. 432–433.Sun SPOT (Sun; Small Programmable Object Technology). (2006, Oct.) [Online]. Available: http://www.sunspotworld.com/

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

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

Margolin, N.B. and B.N. Levine, 2008. "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany: Sprnger.

Luis, V.A., B. Manuel, L. John, 2008. "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 294–311.

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

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

Capkun, S., J.P. Hubaux, L. Buttyan, 2006. "Mobility helps peer-to-peer security," IEEE Trans. Mobile Comput., 5(1): 43–51.

Piro, C., C. Shields, B.N. Levine, 2006. "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 1–11.

Frias-Martinez, V., S.J. Stolfo, A.D. Keromytis, 2009. "BARTER: Behavior profile exchange for behavior-based admission and access control in MANETs," presented at the Proc. 5th Int. Conf. Information Systems Security, Kolkata, India, 193–207.

Buchegger, S., C. Tissieres, J.Y.L. Boudec, 2004. "A test-bed for misbehavior detection in mobile ad-hoc networks: How much can watchdogs really do," in Proc. 6th IEEE Workshop Mobile Comput. Syst. Appl., Dec., 102–111.