IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

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

Divya[1], N.Aparna[2]

[1]Student, Department of CSE, Arcot Sri Mahalakshmi Womens College, Vellore, Tamilnadu, India

[2]Assistant Professor, Department of CSE, Arcot Sri Mahalakshmi Womens College, Vellore, Tamilnadu, India

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 need the solution to be defined. One among the attack is Sybil, on which the identity of the nodes is 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.

CHAPTER 1

Introduction

A Mobile Ad hoc NETwork (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

MANET has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. 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.

Message routing is a problem in a decentralized environment where the topology fluctuates. While the shortest path from a source to a 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 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.

A mobile ad hoc network is an infrastructure less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Figure 1.1 Illustrates the architecture of MANET. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

security attacks like worm hole, black hole, rushing attack , Sybil attack etc.

CHAPTER 2

Literature Survey

2.1 THE SYBIL ATTACK

In this paper the author has proposed a novel method for the detection of Sybil nodes called the Resource Testing Method. Resource Testing is the most commonly implemented solution to averting Sybil attacks. The basic principle is that the quantum of computing resources of each entity on the network is limited. In this approach various tasks are 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.

In this method, a verifier checks whether each identity has as many resources as the single physical device it is associated with. Any discrepancy indicates the possibility of a compromised node. Storage, computation and communication were initially proposed as resources. However, for a system such as a wireless sensor network, an attacker might have storage and computation resources in large capacities compared to resource-starved sensor nodes. Alternatively, verification messages for verifying communication resources might flood the entire system itself. Hence, all three are inadequate choices for sensor networks.

Radio resource testing, is an extension of the resource testing verification method for wireless sensor networks. The key assumptions of this approach are that any physical device has only one radio and that this radio is incapable of transmitting and receiving messages on more than one channel at any given time. Resource tests have been suggested by many as a minimal defense against Sybil attacks where the goal is to reduce their risk substantially rather than to eliminate it altogether.

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

Drawbacks: There are mainly two disadvantages of this approach; firstly, in several applications very little Sybil identities are needed to launch an efficient Sybil attack. Secondly, the intruder can get hold of network resources like storage, network card, memory etc to complete malicious tasks

2.2 A SURVEY OF SOLUTIONS TO THE SYBIL ATTACK

the authors proposed a technique called the Recurring Costs and Fees technique for detecting the Sybil attacks in MANETs. In this approach, identities are periodically re-validated in the network. Each participating identity is periodically or one-time charged with a fee. This method is a variation of 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.

In this approach Margolin proposed a recurring fee per participating identity in order to deter Sybil attackers and they suggest that recurring fee is a stronger deterrent than a one-time fee. The recurring fee may not be a monetary based payment mechanism, but it can also be a nonmonetary payment mechanism such as CAPTCHAs , charged SMS messages, or cooperation in the network. This in itself may be inadequate in controlling the attack since a malicious user incurs only a one-time cost (for computing resources) that may be recovered via the execution of the attack itself, as pointed out by Levine et al. Here the authors make use of an economic model to propose a critical value that exists for a particular combination of application domain and attacker objective. An attack is deemed successful only if ratio of the attacker's objective value to the cost per identity exceeds this critical value. They conclude that using recurring costs or fees per identity is more effective as a deterrent to Sybil attacks than a one-time resource test.

Drawbacks: 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

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

2.3 THE SYBIL ATTACK IN SENSOR NETWORKS: ANALYSIS AND DEFENCES

proposed a novel idea to detect the Sybil Nodes which is called as the *Trusted Devices method.* In a defense related to trusted certification authorities, entities in an application can be linked in some secure fashion to a specific hardware device. This is a one-to-one mapping of a hardware device and a network entity. In other words, one hardware device, such as network card is bound to a single network entity. However, there is no way of preventing an entity from obtaining multiple hardware devices, for example in a scenario in which an attacker installs two network cards. Analogous to any central authority handing out cryptographic certificates, 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.

Similar to the idea of trusted certification, 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.

2.4 MOBILITY HELPS PEER-TO-PEER SECURITY

proposed a technique which exploits the mobility to enhance security in MANETs. In a fully self-organized MANETs where there is no central authority, nodes establish security associations purely by 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

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

the assumption that nodes are connected through wired or infrared connections.

In this paper, 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

2.5 DETECTING THE SYBIL ATTACK IN MOBILE AD HOC NETWORKS

the authors proposed a new technique 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.

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

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.

CHAPTER 3

SYSTEM REQUIREMENTS

HARDWARE CONFIGURATION

Processor	-	Pentium –IV
Speed	-	1.1 Ghz

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

RAM	-	256 MB(min)
Hard Disk	-	20 GB

SOFTWARE CONFIGURATION

Operating System	-	LINUX
Tool	-	Network Simulator-2
Front End	-	OTCL (Object Oriented Tool Command Language)

CHAPTER 4

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. Towards 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.

4.1 Disadvantages of Existing

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

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

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 (Internet Corporation for Assigned Names and Numbers) can be sufficient for Sybil resistance if they are mindfully used. Figure 3.1 depicts the scenario of Sybil attack with multiple identities.

ARCHITECTURE

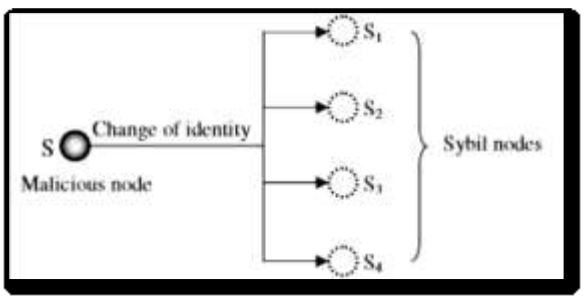


Figure 4.2 Architecture

CHAPTER 5

PROPOSED SYSTEM

The authors proposed a semi-supervised learning approach called SYBILBELIEF. The goal is to propagate reputations from a small set of known benign and/or Sybil users to other users along the social connections between them. More specifically, a binary random variable is associated with each user in the system; such random variable represents the label (i.e., benign or Sybil) of the user. Second, the social network between users in the system is modeled as a pair wise Markov Random Field (MRF), which defines a joint probability distribution for these binary random variables. Third, given a set of known benign and/or Sybil users, the posterior probability of a user being benign is inferred, which is treated as the reputation of the user. For efficient inference of the posterior probability, the Loopy Belief Propagation framework is used , an iterative algorithm for inference on probabilistic graphical models.

5.1 ADVANTAGES OF PROPOSED

The Sybil detection problem is defined as follows. The social network model is introduced with a few design goals.

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

➢ **Social Network Model**

Let us consider an undirected social network $G = (V, E)$, where a node $v \in V$ represents a user in the system and an edge $(u, v) \in E$ indicates that the users $u \in V$ and $v \in V$ are socially connected. In an ideal setting, G represents a weighted network of trust relationships between users, where the edge weights represent the levels of trust between users. Each node is either *benign* or *Sybil*. Figure 3.2 shows the illustration of Sybil attack in a static network. The sub network including the benign nodes and the edges between them are considered as the *benign region*, the sub network including the Sybils and edges between them as the *Sybil region*, and the edges between the two regions as *attack edges*.

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, two techniques are proposed for the efficient detection of Sybil nodes known as the Received Signal Strength (RSS) and the Trusted Key (TK) techniques. Also a prevention mechanism called the Centralized Validation Technique (CVT) is proposed for preventing the Sybil attacks in MANET.

CHAPTER 6

MODULES

6.1 Received Signal Strength Method

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**

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

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 newcomers, if greater than the threshold imply abnormal entry into the neighborhood.

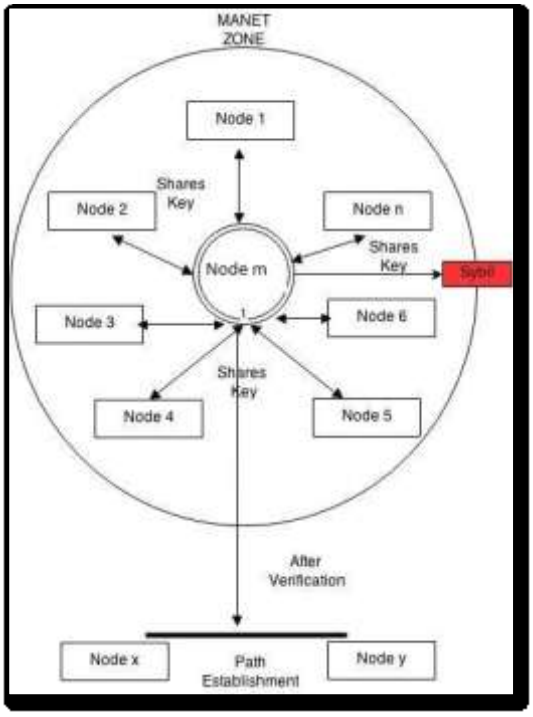
➢ **Algorithm**

In order to detect new identities spawned by a Sybil attacker, the algorithm checks every received RSS by passing it to the addNewRss function, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with before, i.e., it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an *UB−THRESHOLD* (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e., whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list. Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it. Finally, the size of the link list is checked, if it is greater than the *LIST−SIZE*, the oldest RSS is removed from the list.

➢ **6.2 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

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363



The architecture diagram of the Trusted Key Method is shown in Figure 4.4. The diagram describes how the nodes share keys with the base station. A key used by a node cannot be shared with other node. A Sybil node is identified by checking the key associated with the node. After verification the nodes with proper keys are allowed for data transmission.

➢ **System Flow Process**

Step 1. The malicious node x_m 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 x_s is a Sybil node's identity then $x_s < x_i$, where x_m is the malicious node, x_s is the Sybil node and x_i is the legitimate node.

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 x_m 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.

Step 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 based on the following facts:

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.

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

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).

Step 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.

Step 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.

6.3 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.

- **Architecture Diagram of CVT**

IJMTARC – VOLUME – IV – ISSUE - 14 – June 2016 ISSN: 2320-1363

The architecture diagram of Centralized Validation Technique is shown in Figure 4.5. This technique checks whether the node possess a valid certification from the third party to participate in the data transmission. the nodes with the certification is only allowed for data transmission. the nodes which does not receive the certificate are considered Sybil nodes and they are prevented from participating in the data transmission.

CHAPTER 7

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

[1] Neil Zhenqiang Gong, Mario Frank, and Prateek Mittal, " Sybil Belief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014

[2] 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.

[3] 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, Oct. 2006.

[4] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences,"

presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.

[5] S. Capkun, J. P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," *IEEE Trans. Mobile Comput.*, vol. 5, no. 1, pp. 43–51, Jan. 2006.

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

[7] V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, "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, 2009, pp. 193–207.

[8] 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.

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

[10] V. A. Luis, B. Manuel, and L. John, "CAPTCHA: Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp. 294–311.

[11] 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.

[12] 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.

[13] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, 2003.

[14] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

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