Detecting Sybil Attack by Using Received Signal Strength in Manets

K. Kayalvizhi[1], N. Senthilkumar [2], G. Arulkumaran [3]
[1] PG Scholar, Vivekanandha College of Engineering for Women.
[2,3] Assistant Professor, Vivekanandha College of Engineering for Women
Tiruchengode, India
Kayalvizhi07@gmail.com

Abstract— **Fully self-organized mobile ad hoc networks (MANETs) represent complex spread systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique discrete 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 synchronized attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of responsibility in the network. In this research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any additional hardware, such as directional antennae or a geographical positioning system. Through the help of wide simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good precision even in the presence of mobility.**

Keywords – Sybil attacks, Mobile Adhoc Network, Detection.

I. INTRODUCTION

The Mobile ad hoc networks (MANETs) have attracted a lot of attentions due to their interesting and promising functionalities including mobile safety, traffic congestion avoidance, and location based services. This project focus on safety driving application, where each vehicle periodically broadcasts messages including its current position, direction and velocity, as well as road information. Privacy is an important issue in MANETs. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. Pseudonym based schemes have been proposed to preserve the location privacy of mobile. However, those schemes require the mobile to store a large number of pseudonyms and certifications, and do not support some important secure functionality such as authentication and integrity.

The centralized key management has some disadvantages. For instance, the system maintenance is not flexible. Another issue regarding the centralized key management is that many existing schemes assume a tamper-proof device being installed in each vehicle. The tamper-proof device normally costs several thousand dollars. The framework to be developed in this paper does not require the expensive tamper-proof device. Here the technique used and develop a secure distributed key management framework. In my framework, the road side units are responsible for secure group private keys distribution in a localized manner. When a vehicle approaches an, it gets the group private key from the RSU dynamically. All mobile which get the group private key from the same RSU form a group. A new issue induced by the distributed key management framework is that compromised RSUs may misbehave in the key distribution procedure.

SCOPE:

A compromised may deliver other mobile group private keys to its accomplice. Then, the accomplice can send messages under the name of other mobile. Therefore develop security protocols for the distributed key management framework, which are capable of detecting the compromised RSUs and their collusion with the

malicious mobile if any. Computation overhead is another critical issue in MANETs. In the safety driving application, mobile broadcast safety messages. Since the group signature is expensive, the computation overhead of each vehicle will become intolerable when the density of mobile is high the authors propose a promising protocol which let mobile verify messages cooperatively by employing probabilistic verification.

However, in order to guarantee efficient cooperation, mobile have to verify at least twenty-five messages within 300ms which is still a heavy computation burden for the on-board unit (OBU) installed on a vehicle. In addition, the impact of packet loss at the medium access control (MAC) layer on security performance is not investigated. In this proposal recommend a more efficient and practical Cooperative message authentication protocol (CMAP) with an assumption that each safety message carries the location information of the sender vehicle (which can be generated by a global positioning system (GPS) device).

SYBIL ATTACKS

Ad hoc network is composed of mobile, wireless devices, referred to as nodes those communicate only over a shared broadcast channel. An advantage of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to nodes outside direct broadcast range. Each node needs a unique address to participate in the routing. Often addresses are assigned as an IP addresses or a unique media access channel (MAC) address. Because all communications are conducted over the broadcast channel, nothing but these identifiers is available to determine what nodes are present in the network.

DETECTING THE SYBIL ATTACK

In the mobile environment, a single entity impersonating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, they must move in unison, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range. Assuming an attacker uses a single-channel radio, multiple Sybil identities must transmit serially, whereas multiple independent nodes can transmit in parallel. The identities established by a Sybil attacker whether represented by IP addresses, MAC addresses, or public keys differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple identities, any particular assumed identity is resource constrained in computation, storage, or bandwidth.

II. DETECTION OF SYBIL IDENTITIES

A. Attack model

There are two flavors of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivations of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network.

In our scheme, we will consider both types of Sybil attacks. The strategy of our detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks. Hence, in this paper, we will refer to the new Sybil identity and whitewash identity (WID) interchangeably.

We assume that the attacker joins the network with its single identity, and that malicious nodes do not collude with one another. We also assume that nodes do not increase or decrease their transmit power. The attackers can get identities by two ways. First, they can fabricate identities (for example, creating an arbitrary identifier). Second, they can use stolen identities, i.e., spoof the identities of legitimate nodes (masquerading) in the network. We assume the first case where nodes can create arbitrary identifiers because in MANETs, there are no restrictions on identity creation.

B. Signal Strength Based Analysis

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. In order to analyze the difference between a legitimate newcomer and Sybil identity entrance behavior, we setup some experiments in the following. Before we start, it is important to explain how each node collects and maintains the RSS values of the neighboring nodes.

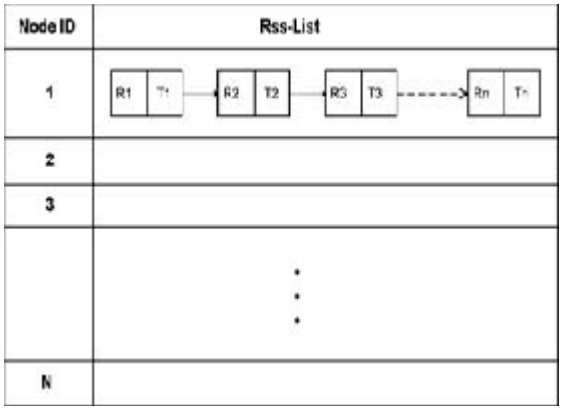
Each node maintains a list of neighbors in the form<Address, Rss-List <time, rss>>, as shown in Table I, and records the RSS values of any directly received or overheard frames of 802.11 protocol, i.e., RTS, CTS, DATA, and ACK messages. In other words, each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when a node either takes part in the communication directly with other nodes acting as a source or a destination or when a node does not take part in the direct communication. In the latter case it will capture the signal strength values of other communicating parties through overhearing the control frames. Each RSS- List in front of the corresponding address contains R_n RSS values of recently received frames along with their time of reception, T_n . Where n is the number of elements in the RSS - List that can be increased or decreased depending upon the memory requirements of a node. In our simulation, we used n to be five elements; however, for real-world scenarios, it should be greater than that because of the time varying nature of RSS.

III. PROPOSED SYSTEM

The proposed system considers both types of Sybil attacks. The strategy of our detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks. Hence, in this paper, I will refer to the new Sybil identity and whitewash identity (WID) interchangeably. I assume that the attacker joins the network with its single identity, and that malicious nodes do not collude with one another. I also assume that nodes do not increase or decrease their transmit power. The attackers can get identities by two ways. First, they can fabricate identities (for example, creating an arbitrary identifier). Second, they can use stolen identities, i.e., spoof the identities of legitimate nodes (masquerading) in the network. I assume the first case where nodes can create arbitrary identifiers because in MANETs, there are no restrictions on identity creation.

In the following experiment, we plot the RSS of nodes in order to determine and visualize the behavior of the new legitimate nodes and the Sybil attackers' new identities.

Table 1 Neighbor list based on RSS



Attack Model

There are two flavors of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivations of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network. In our scheme, we will consider both types of Sybil attacks. The strategy of my detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks.

1) *Experiment 1:* This experiment is designed to allow us to compare the behavior of new legitimate nodes with new Sybil identities. As shown in Fig. 1(a), When a new node *B* enters into another node *A*'s neighborhood or radio range, node *B* gradually enters over time. This is the natural behavior of nodes entering into one another's radio ranges and becoming neighbors in mobile environments. Due to this natural behavior of entrance and exit, when node *A* stays static and node *B* entering into *A*'s radio range with speed *s*, node *A* will observe its RSS continuously increasing. When *A* plots *B*'s RSS readings, *B* moves toward *A* and then ultimately goes out of range on the other side, assuming that *B* is continually communicating with another node *C* or *A*. In graphical form, the RSS of *B* will produce more or less a complete elliptic curve, as shown in Fig. 2. The diagram shows RSS plots for several arbitrary nodes in a random mobile scenario (this is taken from our simulation work presented in Section VI). The interesting characteristic of these plots is that the curve for each legitimate new node starts from the smallest readable RSS value (in an ideal situation), in this case it is good identity (GID) 17 indicating that GID 17 entered into 36 node's radio range normally. Whereas Sybil identities start from higher RSS values, such as WID 6 and 8 indicating that WID 6 and WID 8 did not enter normally into radio ranges of node 36 and node 21, respectively. So it can be deduced that these identities are the whitewashed one and their previous identities were roaming deep inside the radio ranges of the receivers, i.e., 36 and 21.

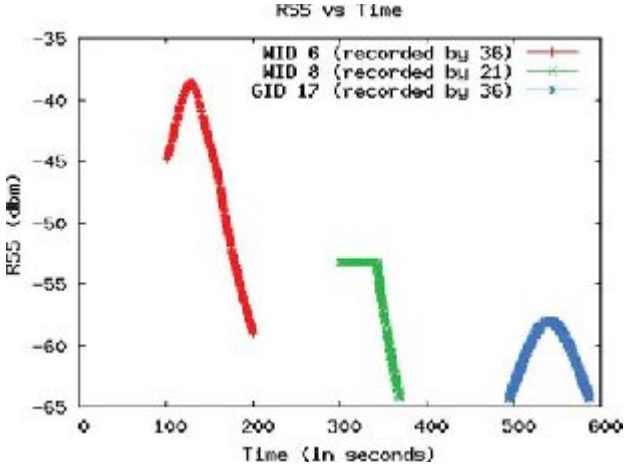


Fig. 1. Plots of three arbitrary nodes' RSS values.

This smallest readable RSS value could be used as a de- tection threshold; however mobility and velocity make things more complicated. For example, the common questions which may arise are, when *A* will receive *B*'s first RSS value and at that particular moment, what would be the location of *B* inside *A*'s radio range? The answer to both of these questions is that it depends on the speed and transmission rate of node *B*. Node with lower transmission rates can penetrate more into the radio ranges before their presence being acknowledged. In other words, the greater the transmission rate of the nodes the sooner (and close to the boundary of radio range) their presence will be acknowledged and vice versa. The greater the speed of *B*, the farther it will penetrate into the radio range of *A* before *A* acknowledges the presence of *B*. In order to refine our detection threshold, we conduct further experiments for speed.

We do not conduct experiment for transmission rate because our aim here is to demonstrate, at what distance node *B* is first acknowledged. This could potentially be affected by speed and transmission rate. We can get our aim by using speed and keeping transmission rate constant (or vice versa).

2) *Experiment 2:* We conducted this experiment in order to establish how far node *B* penetrates into node *A*'s radio range before *A* acknowledges *B*'s presence. For this purpose, we simulate the same scenario as shown in Fig. 1(a) using NS-2.30. First, *A* establishes a connection with *B*, where both the nodes are static. Then, *B* starts moving in the outward direction at a speed of 2 m/s speed until it goes out of range. After taking a pause, node *B* starts moving toward its original location with four different speeds, i.e., 2, 4, 10, and 15 m/s. The resulting RSS values received at node *A* can be seen in Fig. 3.

It is evident from the graphs that the greater the incoming speed of *B*, the greater the first RSS value of *B* that will be received by *A*. In other words, as the incoming speed of *B* increases, it penetrates deeper into *A*'s radio range before *A* acknowledges its presence. Hence, the first presence or RSS signal varies with speed for constant packet transmission rate.

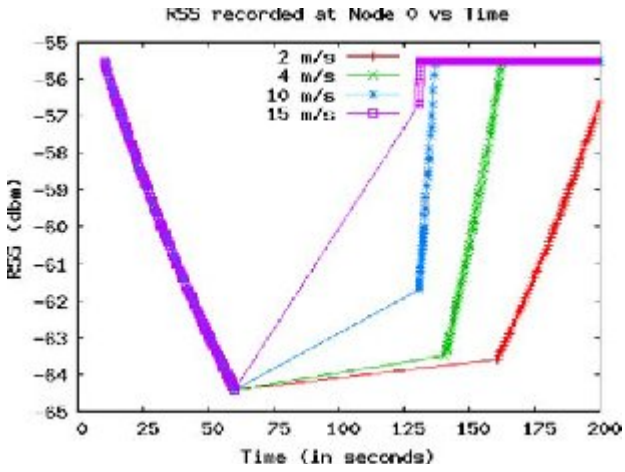


Fig. 2. Determining node presence with respect to different speeds.

IV. TUNING THE THRESHOLD

The main difference we found between the results obtained from our simulations and from our test bed experiments is the variation in RSS values. As RSS varies, for a node *B* at a fixed distance *d* from a node *A*, the receiving node *A* can receive multiple different RSS values in the fluctuation range $[-v, +v]$ (assuming $+v$ is greater than $-v$) and hence these values do not represent an *exact* indication of distance. The detection threshold will be affected when it works based on a single RSS value. For example, node *A* can receive RSS from *B* at any particular time while *B* is a good node just outside the white zone of *A* with $+v$ variance, the position of *B* can be shown in Fig. 13(a). As a result, due to the $+v$ variation in the RSS, *A* will consider *B* to be a new identity emerged in its white zone, and hence node *B* will incorrectly be detected as a Sybil identity. As shown in Fig. 13(b), another case can occur when node *B* is a whitewasher in the white zone near the boundary performs a whitewash, however, due to the variations in signal strength node *A* might receive RSS with $-v$ variation, considering it a signal coming from its gray zone and hence will consider *B* as a good node. One way of mitigating the effect of this variation is to base our detection on an average RSS across *n* values (moving average), instead of basing our detection on a single RSS value. Before we tune the threshold, it is important to determine the real –world fluctuation in RSS. For this purpose, we conducted a test bed experiment using Sun SPOT.

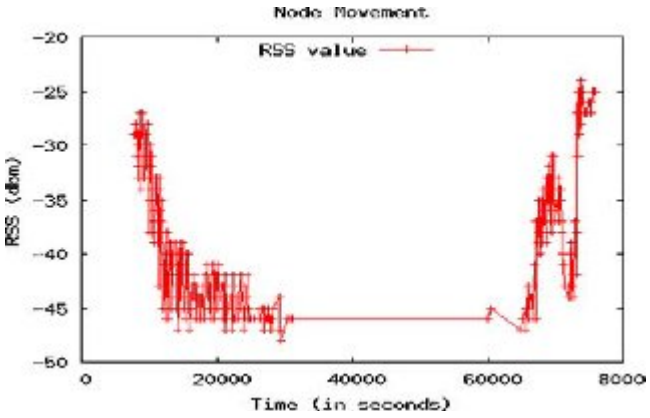


Fig. 3. Using robot, node movement with same in/out speed.

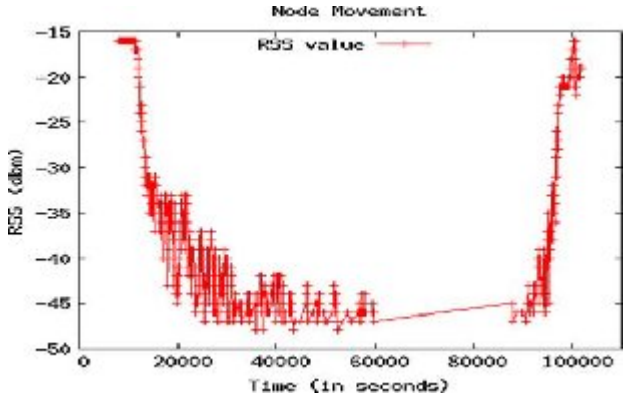


Fig.4. Using robot, node movement with different in/out speed.

We will tune our detection threshold based on the speed and variation of the RSS values. This threshold logically partitions the radio range into white and gray zones: greater (or equal) signal strength than the threshold means the signal is emanating from the white zone and from the gray zone otherwise. Let node *B* be approaching node *A*'s radio range with velocity *s* (m s−1), assuming that *d*b is the boundary of *A*'s radio range (in meters), _*t* is the time (in seconds) between two packet transmissions and *dv* is the inaccuracy in distance caused by *v* (in meters), where *v* is the variation in the RSS in the range of [−*v*, +*v*]. We assume for the sake of simplicity that just before the boundary, *B* transmits a packet which is not captured by *A*.

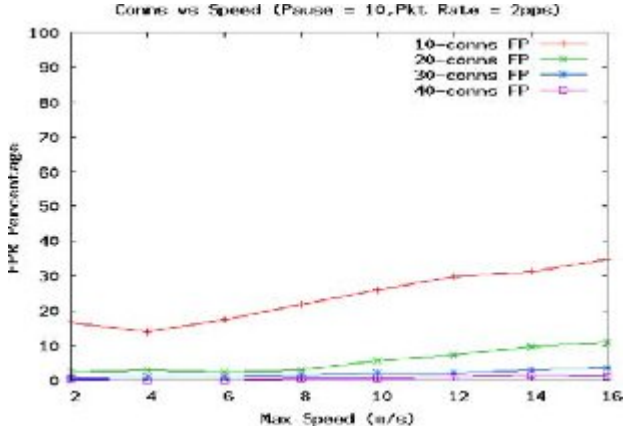


Fig.5. False positives with various speeds and connections.

So the next transmitted packet of *B* that *A* will capture as a first acknowledgment of *B* will become the worst case white zone, can be calculated as follows:

$$ZW = (db + dv) + (s \times \_t). \quad (1)$$

The value of *dv* and *s* will be negative when node *B* is moving toward node *A* and positive otherwise. From Appendix we can know the value of *db* is approximately 10m and variance *v* at the boundary is 2.24 dbm which is the two standard deviation (SD), shown in Table V. Now in order to find out *dv*, ~~we~~ do the following computations The power received at any distance *d* is inversely proportional to the *m*th power of the distance [25], that is where *Pd* is the received power at distance *d* and in free space anzd in line-of-sight conditions, the path loss exponent *m* is 2.

IV. SIMULATION SETUP AND EVALUATION

In order to implement and evaluate our scheme, we use Network Simulator NS-2.30 using the parameters listed in Table II. The *UB−THRESHOLD* is the averaged RSS value (in Watts) of several scenarios when a transmitter is moving with 10 m/s speed; lower speeds thresholds will improve detection accuracy, as discussed in Section III-C. The *TIME−THRESHOLD* is the average (maximum) time in which a node should listen from another node, otherwise that identity will be considered as out of range or previous identity of a whitewasher. Shorter time intervals will increase identity revalidations in the network; whereas lengthy intervals will increase table sizes in network nodes. The *LIST−SIZE* is the maximum RSS records retained for an identity or address. We used 5 as an arbitrary number of records per identity; however, it can be increased depending upon the memory capacity of nodes. In this simulation study our aim is to establish the detection percentage of our proposed scheme in different scenarios. As we discussed above, there are some attributes of the network that are mainly responsible for affecting the accuracy of our Sybil attack detection scheme. These attributes are number network connections, node density and transmission rate. In each of our scenario we take speed as our main attribute.

All of the results we present here have been calculated as an average of 25 different random scenarios (or simulation runs). In the following subsections, we will discuss our metrics and will analyze our simulation results that are based on a
variety of node speeds, packet transmission rates, connections and node densities.

A. Metrics

We use two main metrics in order to determine the detection accuracy of our scheme in different environments, i.e., true positive rate (TPR) and false positive rate. True positive means a malicious node is correctly detected and false positive means a good or legitimate node is incorrectly detected as a malicious.

B. Analysis

As shown in figure data connections in the network are inversely proportional to the false positives of our scheme. For detection, movement sensing or the reception of frequent RSS values are important. In order to obtain RSS values from a node, that node should be involved in some form of communication, for example by acting as a source, forwarder, or destination. The more frequently a node sends or receives packets, the more efficiently a neighboring node will detect
it in the event that it tries to create its Sybil identity. Fewer connections in a network imply fewer source and destination nodes, and greater difficulty for a node to distinguish other nodes' positions (i.e., their position as being either in a gray or white zone). Consequently a greater number of false positives will result. However, connections have no apparent effect on the true positives and for most of our experiments the true positives remained around the 90% level, as depicted

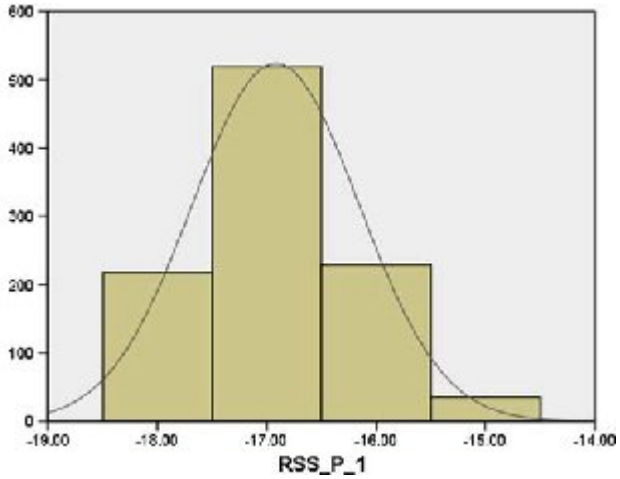


Fig. 6. Data distribution for 1-ft distance.

V. CONCLUSION

In this paper, we proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. We demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities. We confirmed this distinction rationale through simulations and through the use of a real-world test bed of Sun SPOT sensors. We also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. The simulation results showed that our scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy.

REFERENCES

[1] 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.

[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] 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.

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

[5] K. Hoeper and G. Gong, "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, 2007.

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

[7] 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.

[8] 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.

[9] 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.

[10] T. Suen and A. Yasinsac, "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. 2005, pp. 432 to 433.