A NOVEL METHOD FOR SECURITY ENHANCEMENT IN MANET

[1]T. SARANYA, [2]A.KUMARAVEL

[1]PG Scholar, Paavai Engineering College, Namakkal.
[2]Assistant Professor, Paavai Engineering College, Namakkal
E-mail: [1]saran.saranya2704@gmail.com, [2]kumaravel.ece2k4@gmail.com

Abstract- Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed 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, 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 research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

Index Terms- Identity-based attacks, intrusion detection, mobile ad hoc networks, Sybil attacks.

I. INTRODUCTION

MOBILE ad hoc networks (MANETs) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies [1]. This allows people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. The unique characteristics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized identity management in MANETs and the requirement of a unique, distinct, and persistent identity per node for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. For example, communications in wireless networks are usually based on a unique identifier that represents a network entity: a node. Identifiers are used as an address to communicate with a network entity. This forms a one-to-one mapping between an identity and an entity and that is usually assumed either implicitly or explicitly by many protocol mechanisms; hence two identities implies two distinct nodes. Unfortunately malicious nodes can illegitimately claim multiple identities and violate this one-to one mapping of identity and entity philosophy. Douceur [2] termed this as a Sybil attack, in which an attacker manages to create and control more than one identity on a single physical device.

A Sybil attacker can cause damage to the ad hoc networks in several ways [3]. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.

II. RELATED WORK

The OLSR protocol is an optimization of the classical Link-State Routing protocol (LSR), aimed at reducing network overhead. While the original LSR uses a flooding propagation technique in which a node receiving any message must retransmit it to all its neighbors, OLSR selectively retransmits messages based on a specified set of rules. The crux of the optimization is based upon a subset of 1-hop neighbors, called multi-point relays (MPR), which are designated as forwarding agents for control packets throughout the network. MPRs are selected by a node as a subset of its 1-hop neighbors, such that the MPR set allows coverage of all of its 2-hop neighbors. By minimizing its MPR selections, a node is able to transmit messages to all 2-hop neighbors with minimal duplication. Thus, both topology control messages and data packets are only forwarded by this minimal MPR set, allowing for fewer duplicate messages while maintaining network-wide coverage. There are two types of messages used to discover

network topology in OLSR: HELLO and TC (i.e., topology control). The HELLO message, which declares a node's knowledge of its surrounding, is broadcast to all. Any node that can hear the broadcast and reciprocate back to the sender is classified as a 1-hop neighbor. Consequently, each node acquires its local topology up to a 2-hop range. In addition, OLSR requires that all nodes selected as MPRs periodically advertise a TC message listing all nodes that have selected the sender as its MPR. These control messages are only propagated through the MPR super-network, reducing overall network traffic. Each node in the network maintains network topology based on both the HELLO and TC messages it receives. It then calculates and stores, for each node discovered, the shortest distance (i.e., the minimal required hops between the source and the destination) between itself and one of the destination's node MPRs; hence, the shortest path to the destination. See [4] for more details.

III. 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 ata 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. The difference between the two is only the notion of simultaneity; however, their applications and consequences are different.

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.

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 Rn RSS values of recently received frames along with their time of reception, Tn. 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.

TABLE I
NEIGHBOR LIST BASED ON RSS

Node ID	Rss-List
1	R1 T1 → R2 T2 → R3 T3 ----→ Rn Tn
2	
3	
⋮	⋮
N	

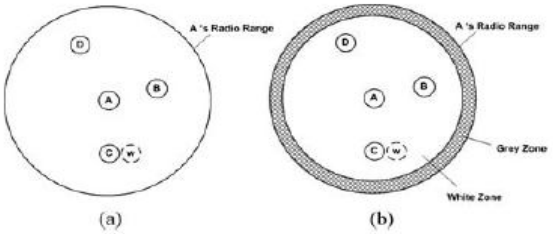


Fig. 1.(a) Without and (b) with categorization of radio range.

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.

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 8did not enter normally into radio ranges of node 36 and node21, 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., 36and 21. This smallest readable RSS value could be used as a detection 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.

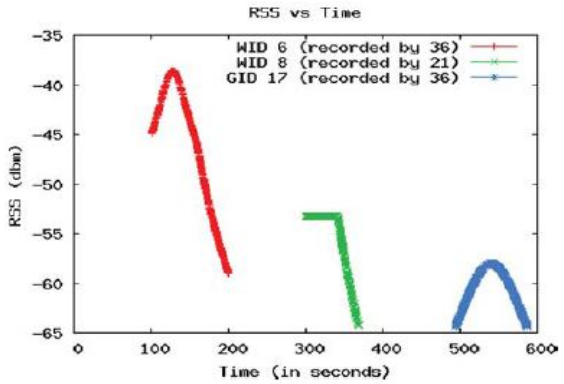


Fig. 2.Plots of three arbitrary nodes' RSS values.

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) usingNS-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 origin allocation 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.

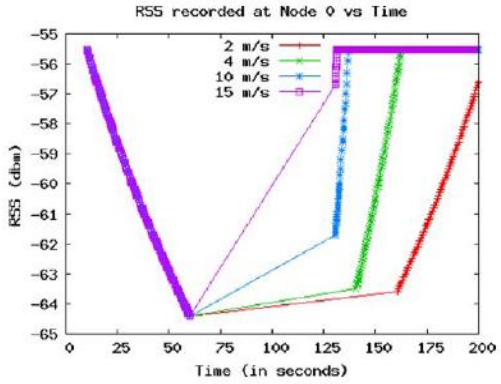


Fig. 3.Determining node presence with respect to different speeds.

IV. TUNING THE THRESHOLD

The main difference we found between the results obtained from our simulations and from our testbed 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 besh own 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.

V. 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 of 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).

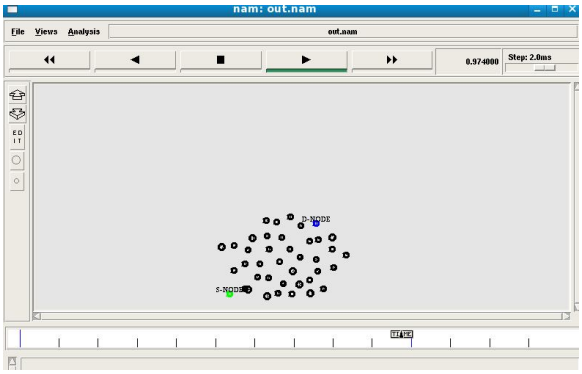


Fig. 4: Source to destination transmission

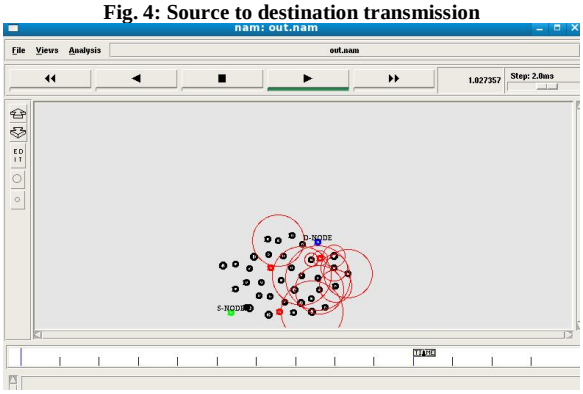


Fig. 5: Node RSS value calculation

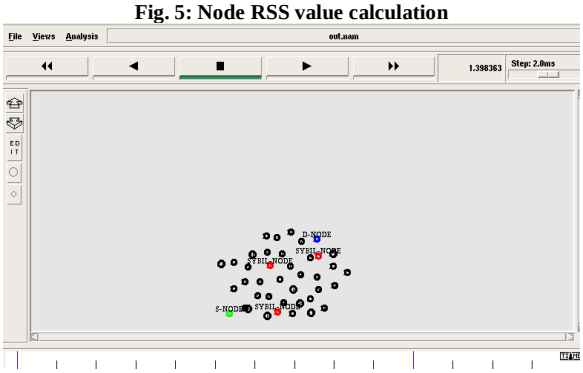


Fig. 6: Sybil node Identification

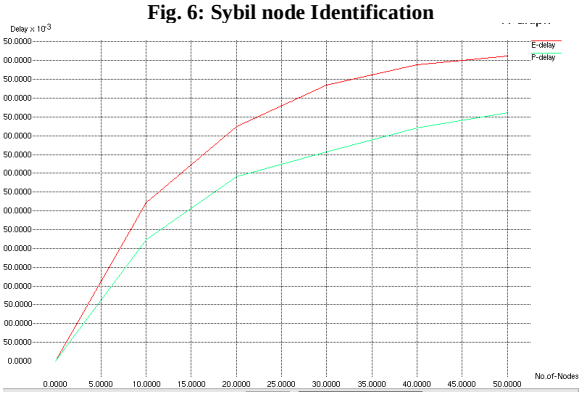


Fig. 7: Delay Analysis (Existing Vs Proposed)

TABLE II

SIMULATION PARAMETERS

Parameter	Level
Area	1000 m × 1000 m
Speed	2 to 16 m/s
Pause time	10 s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 m
Carrier sense range	550 m
Number of nodes	20 to 60
MAC	802.11
Application	CBR, 10 to 40
Packet size	64 B
Simulation time	600 s
Movement	Random Waypoint model
Placement	Uniform
Malicious population	10%
Sybil Ids per malicious node	5
RSS_TIMEOUT	100 s
TIME_THRESHOLD	30 s
UB_RSS_THRESHOLD	6.45×10^{-10} W
LIST_SIZE	5

CONCLUSION AND FUTURE WORK

In this paper, we proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks. The 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. 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. Our future work includes tackling issues related to variable transmit powers and masquerading attacks in the network.

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,” inProc. 4th Workshop Hot Nets, 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, "Sybilnodes detection based on received signal strength variations withinVANET," 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] A. Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, Robust Sybil detection for MANETs," in Proc. 18th ICCCN 2009, pp. 1–6.

★★★