EFFICIENT WAY TO DETECT SYBIL ATTACK AND DENIAL OF SERVICE ATTACK IN MANETs

Vishnu Paarkavi.K[1], Vignesh.C[2], Suganya.J[3]

Department of Computer Science and Engineering
SNS college of technology, India
[1]vishnu_8@yahoo.com
[2]vignesh.vs1215@gmail.com

Guided by,
Kavitha.M
Assistant Professor
Department of Computer Science and Engineering
SNS College of Technology, India
tameezh@yahoo.co.in

Abstract- **Mobile ad hoc networks consist of a collection of mobile nodes without having a fixed infrastructure. Due to the lack of centralized identity management in MANETs, 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 the light weight Sybil attack detection scheme, in order to differentiate the legitimate and Sybil nodes the received signal strength is utilized. But in this method, only Sybil attack is detected. But in MANET there are some more attacks. Denial-of-Service (DoS) attacks are a major class of threat today. Two of the most common DoS attacks are Gray hole and Black hole attacks in MANET. So, in order to overcome this problem, a new detection mechanism is introduced to detect the gray hole and black hole attacks. In this mechanism, an intermediate node receiving abnormal routing information from its neighbor node considers that neighbor node as a malicious node. Experimental results show that the proposed system detects the gray hole and black hole attacks in high detection accuracy.**

Keywords**: Sybil attack, Gray hole, White hole, Received Signal Strength, Ad hoc.**

I. INTRODUCTION

MANET stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless devices, while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network) is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

II. RELATED WORKS

The Sybil Attack in Sensor Networks: In this work, to investigate the Sybil attack, a particularly harmful attack in sensor networks. In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device. This is the first work that systematically analyzes the Sybil attack and its defenses in sensor networks. This work makes the following contributions. To introduce taxonomy of the different forms of the Sybil attack as it applies to wireless sensor networks. To analyze how an attacker can use the different types of the Sybil attack to perturb or compromise several sensor network protocols. To propose several new defenses against the Sybil

attack, including radio resource testing, key validation for random key pre-distribution, position verification, and registration. Through quantitative analysis, we show that the radio resource testing method is very effective given the assumption that a malicious node cannot send on multiple channels simultaneously.

Sybil Nodes Detection based on Received Signal Strength Variations within VANETs: A Sybil detection technique based on physical signal characteristics, easily measurable by the commonly used wireless cards. This technique allows detecting malicious and Sybil nodes within VANETs by using received signal strength variations, localization verification and nodes distinguishability degree evaluation. By measuring the received signal strength variations, we obtain an estimation of relative nodes localization. This rough localization gives an accurate enough indication on how much a pair of nodes could be distinguished from each other, known as "the distinguishability degree". The geographical localization technique takes into account the characteristics of the wireless networks, such as mobility and dynamicity of nodes, assuming that all messages are sent with the same signal strength, which is not particularly constraining as a Sybil attacker emitting with constant power level has more chances to remain covered up.

Radio Resource Tests: The Sybil Attack is a relevant threat to the secure and dependable operation of wireless ad hoc networks. It consists in having a malicious node simultaneously assuming multiple identities, commonly called Sybil identities. Such a node can easily disrupt the operation of distributed protocols, such as distributed storage, routing, data aggregation, voting, intrusion detection, and resource sharing. A radio resource test (RRT) is a technique that allows detection of Sybil identities and therefore, is a fundamental building block for developing dependable architectures for wireless ad hoc networks. RRTs are a particular case of the more general class of arbitrary resource tests. Resource tests operate under the assumption that it is possible to establish a bound to the resources available to a single node. Two non-Sybil identities must, therefore, be capable of demonstrating that they own more aggregate resources than those available to a single node. Different kinds of resources can be tested, including computational power, storage capacity, and network bandwidth. RRTs assume that each node has access to a single radio device and builds upon the limitations of these devices. RRTs have the potential to support protocols that do not require pre-configuration, nor pre-shared secrets, improving the scalability of the network. This paper makes the following contributions: propose a framework to assess the power and performance of RRTs; we propose a number of novel RRTs; we make a comparative analysis of different RRTs; to discuss how these tests can be used to test a population of identities, and determine the cost of such combined test.

CAPTCHA: To introduce CAPTCHA, an automated test that humans can pass, but current computer programs can't pass: any program that has high success over a CAPTCHA can be used to solve an unsolved Artificial Intelligence (AI) problem. An important component of the success of modern cryptography is the practice of stating, very precisely and clearly, the assumptions under which cryptographic protocols are secure. This allows the rest of the community to evaluate the assumptions and to attempt to break them. In the case of Artificial Intelligence, it's rare for problems to be precisely stated, but using them for security purposes forces protocol designers to do so. To believe that precisely stating unsolved AI problems can accelerate the development of Artificial Intelligence: most AI problems that have been precisely stated and publicized have eventually been solved.

PASID: In this work, to show that the mobility of nodes in a wireless network can be used to detect and identify nodes that is part of a Sybil attack. To 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. To propose 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, this helps reveal Sybil attackers. The second method, PASID with Group Detection (PASID-GD), extends our approach and reduces false positives that can occur when a group of nodes moving together is falsely identified as a single Sybil attacker. 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.

III. EXISTING SYSTEM

In the existing System, in order to detect the Sybil attacks a lightweight scheme is used for detecting new identities of Sybil attackers without using centralized trusted third party or any extra hardware. Because due to 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. A Sybil attacker can cause damage to the ad hoc networks in several ways. 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. This scheme utilizes the received signal strength (RSS) in order to differentiate between the legitimate and Sybil identities. Firstly, to demonstrate the entry and exit behavior of legitimate nodes and Sybil nodes. Secondly, to define a threshold that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior. Third, tune the detection threshold by incorporating the RSS data fluctuation. The scheme can be applied to both scenarios of Sybil attacks, i.e., whether the new identities are created one after the other or simultaneously make no difference to the detection process. This detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes, for example it could be incorporated into a reputation-based system, i.e., the detected Sybil identities from the MAC layer will be plugged into the reputation-based system on network layer. The proposed scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment. Unlike proposed scheme does not use centralized trusted third party. In this scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner.

IV. PROPOSED SYSTEM

In the proposed system, in order to detect the DoS attacks a new detection scheme is proposed. But in MANET there are some more attacks. In the existing system only consider the Sybil attack. So, in the proposed system also consider Denial of service attacks. Denial-of-Service (DoS) attacks are a major class of threat today. Two of the most common DoS attacks are Gray hole and Black hole attacks in MANET. In Black hole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed. Gray hole attack is an extension of Black hole attack in which a malicious node's behavior is exceptionally unpredictable. A node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Both Black hole and Gray hole attacks disturb route discovery process and degrade network's performance. In this proposed mechanism, an intermediate node receiving abnormal routing information from its neighbor node considers that neighbor node as a malicious node. The intermediate node appends the information about the malicious node in the route reply packet and every node receiving that reply packet then upgrades its routing table to mark the node as malicious node. When routing request is sent, a list of malicious node is appended to the packet and every node receiving the packet upgrades its routing table to mark the listed nodes as malicious. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then tells other nodes not to consider the routing information received from the malicious node.

V. DETECTION OF SYBIL NODE

A. *Analysis of received signal strength*

A network is created with mobile nodes. Each node covers a particular range of network. Based on the neighborhood joining behavior, the distinction between a new legitimate node and a new Sybil identity is identified. If 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. Every node maintains a list of neighbors in the form <Address, RSS-list, <time_rss> and records the RSS values. Each RSS list in 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. A threshold value is calculated as the average of the speed of the nodes. The RSS value is used to find Sybil node.

B. *Detection of Sybil nodes*

To set the detection threshold, based on the maximum speed of the network. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighborhood. Partition the radio range of node into two zones: a gray zone and a white zone. This partitioning is based on the speed-based detection threshold. It would become clear that higher speed thresholds produce wider gray zones. A node in the gray zone would usually represent a normal entry into the radio range of the node. So any new identity creation in the white zone will be detected as a whitewashing or Sybil identity, because normal nodes cannot produce their first appearance in this area. If the first RSS value captured is greater than the threshold, i.e., a node is in the white zone, *A* will deem that identity as a new identity from a Sybil attacker, since no node can penetrate into white zone within the specified speed. If the first RSS value received is less than the threshold, i.e., a node is in the gray zone, it will be considered as a normal new entrant and will be added to the neighbor list. Upon detection of Sybil identity, the detector node will inform its 1-hop neighbors by transmitting a special detection update packet. Each node when receives two or more than two packets from two distinct nodes about an identity to be Sybil, that identity will be deemed as Sybil identity.

Algorithm:
addNewRss (Address, rss, time_recv)
BEGIN SUB:
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:

VI. DETECTION OF DDOS

In this method, an intermediate node receiving abnormal routing information from its neighbour node considers that neighbour node as a malicious node. The intermediate node appends the information about the malicious node in the route reply packet and every node receiving that reply packet then upgrades its routing table to mark the node as malicious node. When routing request is sent, a list of malicious node is appended to the packet and every node receiving the packet upgrades its routing table to mark the listed nodes as malicious. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then tells other nodes not to consider the routing information received from the malicious node. Thus in AODV protocol, when a node receives a route reply packet (RREP), it checks the sequence number value in routing table; if it is greater than the one in the RREP, the RREP packet is accepted; otherwise it is discarded.

Algorithm:

1. Source Node broadcasts Route Request packet
2. Intermediate node receives a packet
3. Calculate Peak Value
4. Peak value= ([(Diff x RFR) + No. of replies received by intermediate node during the time interval +Current Simulation time])/3
   //Diff = Difference between routing table sequence number and route reply sequence
   // RFR= Reply Forward Ratio
   // Simulation time = Elapsed time of adhoc network
   If seqno >peak value **then**
5. Marked as DO_NOT_CONSIDER
6. **Else**
7. Accept the packet
8. **Endif**

VII. DETECTION OF DDOS

Finally, in this section the existing and the proposed system is compared and evaluated. In the existing

system, 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. In the proposed system, to detect the DoS attacks, a new detection scheme is proposed. When compared to the existing system, to achieve high detection ratio in the proposed system.

VIII. CONCLUSION

An RSS-based detection mechanism is used 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 and through the use of a real-world testbed 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. In addition to that, to detect the DoS attacks in the mobile adhoc networks, a new detection scheme is proposed. The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets.

IX. FUTURE WORK

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

[11] 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. 432–433.

[12] *Sun SPOT (Sun; Small Programmable Object Technology)*. (2006, Oct.) [Online]. Available: http://www.sunspotworld.com/

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

