Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Detecting Sybil Attack By Using Received Signal Strength In MANETS

Ms. M. Dharika IInd M.E./CSE
Mrs .S. Prema M. E., AP / ECE
Mahendra Institute of Technology, Namakkal , Tamilnadu, India

Abstract-Fully self-organized mobile adhoc 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, 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 is proposed. Through the help of extensive simulations and real-world testbed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts and military networks. Such network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links [6]. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes they, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling and routing. Determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

The concepts and operational requirements associated with the current idea of MANETs are discussed in the mobile computing and networking literature, notably documents and standards developed by the MANET Working Group of the Routing Area of the Internet Engineering Task Force (IETF).

II. KEY ISSUES AND CHALLENGES

There are several keys issues and challenges

2.1. Link Level Security

In wireless environment the links are susceptible to attacks where eavesdropper can easily spoof the ongoing communication. As there is no protection like firewalls or access control in Ad-hoc network any node can become vulnerable to attacks coming from any direction or from any node. The results of such attacks include spoofing of the node's identity, tampering with node's credentials, leaking of confidential information or impersonating node.

2.2. Security Factors

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, consider the following attributes: availability, confidentiality, integrity, authentication and non-repudiation. Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences [7]. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

2.3. Key Management

In general, security goals in ad hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature. These mechanisms are supported through centralized key management where trusted Certificate Authority (CA) provides public key certificate to mobile nodes so nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network. The proposed mechanisms used for identification such as shared secret, public key cryptography, third party authentication provide partial solution, as they are vulnerable or unable to scale. All proposed solutions require that the mobile users make proper usage of cryptographic keys. Goal of proper management and safekeeping of small number of cryptographic keys is difficult to achieve in ad hoc network due to random mobility of nodes where continuous connectivity is not maintained.

III. RELATED WORK

Levine *et al. s*urveyed countermeasures against Sybil attacks and categorized these techniques as follows.

Resource Testing: In this approach [4], 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. The drawback of this approach is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks.

Recurring Costs and Fees: In this approach, identities are periodically re validated in the network. Each participating identity is periodically or one-time charged with a fee. For example, Margolin *et al.* [9] 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 [3].

Trusted Devices: Piro *et al.* proposed to detect Sybil identities by observing node dynamics. Nodes are keeping track of identities which are often seen together (Sybil identities) as opposed to the honest distinct nodes that move freely in different directions. However, the scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target. BARTER [1] is a behavior-based access and admission control system for MANETs in which nodes initially exchange their behavior profiles and calculate individual local definitions of normal network behavior. During admission, each node issues an individual decision based on its definition of normalcy. These individual decisions are then combined via a threshold cryptography that requires agreement among a fixed amount of MANET nodes to change the status of the network.

IV. DISCOVERING SYBIL ATTACK UNDER MANETS

A Sybil attacker can cause damage to the ad hoc networks in several ways. 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.

Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification [5], [6]. This approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks [7], [8]. This approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).

In this paper, we will present our scheme that detects Sybil identities. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behavior of legitimate nodes and Sybil nodes using simulation and testbed experimentation. Second, we define a threshold that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior. Third, we tune our detection threshold by incorporating the RSS data fluctuation taken from our testbed experimentation. Fourth, we evaluate our scheme using extensive simulations, and the results show that it produces about 90% true positives and about 10% false positives in mobile environments. 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. Our 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. Our proposed scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment, as used in [8]. Unlike [10], our proposed scheme does not use centralized trusted third party. In our scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner.

V. PROBLEM STATEMENT

In existing system, hackers easily can act as source node and sends message to destination. Destination receives wrong message from hackers. Destination believes that its correct message from source. Destination receives the wrong information from hackers. Messages are passed from sender to destination without any security. 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. Message header holds source node information which sends the message to receiver. Hackers can easily change that header information and sends to destination. They have much loss of data and not a secure process on the network.

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. The following problems identified from the existing system.

- Destination gets the wrong information from hackers or malicious user.
- There is no any server to detect hackers.
- Overhead of packet loss
- Low level network performance

VI. RECEIVED SIGNAL STRENGTH BASED SYBIL ATTACK DETECTION SCHEME

In this proposed system, hackers cannot act as source, because one centralized server is maintaining to check authentication of source. It blacks unauthorized users or hackers. We have to provide a key based data transmission and id based network. Passive ad hoc identity like a Route based packet filter node to watch the transmission on the network. Our proposed system used the Route Based Packet Filter Algorithm. Use these algorithms to transfer the data in source to destination without any damage or loss as well as each node to have the neighbor's node address. Depends on the address the data will be transmitted in to correct destination. If they have any packet loss are some collision on network immediately to inform the server to stop the data and maintaining source node information and header information of message. It checks the users using those details whether they are attackers or normal user. Hacker's information has not been transferred to destination. Destination has not been receiving any attacker information. In our proposed method to use secure and avoid the attacking system on the network.

Route Based Packet Filter Algorithms:

Step 1: Each node to know the neighbors node address.

Step 2: If neighbor's node is centralized server node means Store data Else, To search the centralized node.

Step 3: The server nodes have all source data as well as destination address.

Step 4: Each node has the individual keys. Depends on the keys the centralized server is to identify the destination address.

Step 5: In RPF algorithm and centralized server method is used to preventing the data in to any attackers

Step 6: The destination node easily to check the data is correct or not.

Step 7: If any attackers damage the data means destinations node again send the data in to centralized server.

6.1. Wireless Network Configures Setting

Wireless mobile ad hoc Networks create a number of nodes. The packets to send and receiving through the source to destination. It's based the scheme of packets delivered for ACK packet drop on the nodes. In this network to creating a source to destination, intermediately set a server or base station on network. Transmit the data processing on their whole networking.

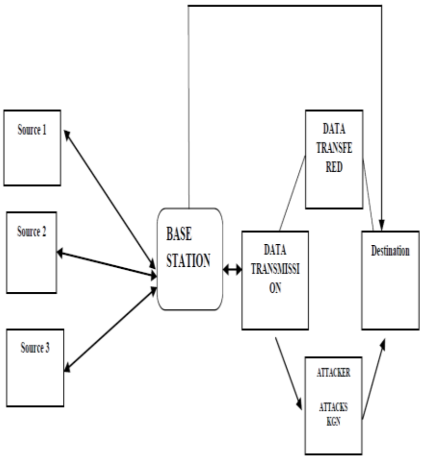

Figure 6.1. Received Signal Strength Based Sybil Attack Detection Scheme

6.2. Topology Design

This module is developed to Topology design all node place particular distance. Without using any cables then fully wireless equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The sink is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology. It creates a geographical representation or arrangements of nodes to choose source and destination for the further transmission of packets in the network.

6.3. Node Creating

This module is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. From Source node to destination node it involves in the selection of neighbor nodes and short path for transmission. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

6.4. Route Based Packet Filter

In these algorithm used to, in our MANET each and every nodes knows the neighbors address. Depends on the address easily transfer the data to destination without any attack or packet loss. Transmission from source to destination each node must have the knowledge of its neighbor node for the packet transmits .This module helps for the choosing its neighbor nodes and its identity for storing in the neighbor table.

6.5. Centralized Server

Centralized server is used to collect the all the data. Also knows the every node key address. Using these key data will be sending the destination without any damage. The packet will be transmitting easily by using this key form source to destination.

6.6. Sybil Attack

The attacker uses different identities at the same time. A single attacker could pretend nodes to report the existence of a false bottleneck in traffic. MANETs are mainly related to illegally gathering sensitive information about mobile nodes. To relate between a source and its destination, effect on data and transmission time on network.

6.7. Random Key Distributor

In this module have to use a random key distribute for an every node on the network. It has more security and efficient data transmission on their network. If they have key means to access the data from the source node on the network.

6.8. Passive Ad Hoc Identifier

In this module 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 on the network. It has using a neighbor nodes list to watch the network collision or any dropping on network.

6.9. Graph Design Based Result

Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, delivery ratio, network delay, energy efficient and etc. In Existing graph only shows throughout and delivery ratio but in proposed it shows its packet delay too.

VII. CONCLUSION

Complete simulation criteria for considering the resolution of specified objectives and their problem reports simultaneously, that is, the behavior of routing protocols in MANETs by considering the realistic attack traces is compromised. The three metrics of PDR, E2D, THROUGHOUT, are evaluated using AODV protocol in three density regions of low density, medium density and high density in network scene as well as in node point. It has to provide a key based data transmission and id based network. Passive ad hoc identity like as Route Based Packet Filter node to watch the transmission on the network. Use these algorithms to transfer the data in source to destination without any damage or loss as well as each node to have the neighbor’s node address. It have any packet loss are some collision on network immediately to inform the server to stop the data and maintaining source node information and header information of message. It checks the users using those details whether they are attackers or normal user. The proposed systems use the RPF Algorithm to secure system and avoid the attacking system on the network. In the future to take a different security based routing protocols and then improves the network performance system.

REFERENCES

[1] 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.

[2] A. Parameswaran, M. I. Husain and S. Upadhyaya, “Is RSSI a reliable parameter in sensor localization algorithms: An experimental study,” in *Proc. F2DA*, 2009.

[3] 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.

[4] 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.

[5] K. Hoeper and G. Gong, “Bootstrapping security in mobile ad hoc networks using identity-based schemes,” in *Security in Distributed and Networking Systems* 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.

[7] Y. Chen, J. Yang and R. P. Martin, “Detecting and localizing identity-based attacks in wireless and sensor networks,” *IEEE Trans. Veh. Technol.*, Jun. 2010.

[8] M. S. Bouassida and B. Ducourthial, “Sybil nodes detection based on received signal strength variations within VANET,” *Int. J. Netw. Security*, vol. 8, May 2009.

[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] A. Tangpong, G. Kesidis, H. Hung-Yuan and A. Hurson, “Robust Sybil detection for MANETs,” in *Proc. 18th ICCCN* 2009.

[11] Gong and Di Wang “On the Security of Trustee-Based Social Authentications” IEEE Transactions on Information Forensics and Security, August 2014