Sybil Attack Analysis and Detection Techniques in MANET

Chakradhar Verma
Research Scholar UCE,RTU, Kota(Raj.)
chakradharverma@gmail.com

Dr. C. P. Gupta
RTU, Kota(Raj.)
guptacp2@rediffmaill.com

Abstract— Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack [6], where a node Illegitimately claims multiple identities.Mobility cause a main problem when we talk about security in Mobile Ad-hoc networks. It doesn't depend on fixed architecture, the nodes are continuously moving in a random fashion. In this article we will focus on identifying the Sybil attack in MANET. It uses air medium for communication so it is more prone to the attack. Sybil attack is one in which single node present multiple fake identities to other nodes, which cause destruction.

Keywords*- MANET, Sybil attack, Fake identity*

*****

I. Introduction

A mobile ad hoc network (MANET), also known as wireless ad hoc network or ad hoc wireless network, is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Mobile Ad-hoc Network: MANET is a combination of sensor node that can proceed on their own and connect with the physical environment. Mobile nodes have the ability of computing, sensing and communication like static nodes.

For mobile nodes, Ad-hoc network is the new technology of wireless communication. Unlike wireless sensor network where are base stations or mobile switching centers, here in MANET the mobile nodes communication directly which are near and those which are far rely message through other nodes.

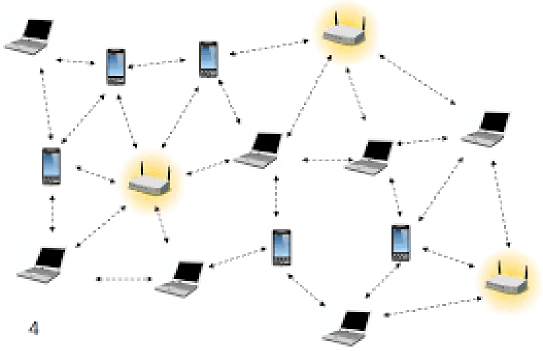

Fig. 1 – MANET Network

Security in sensor networks is complicated by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware (to keep per-node costs low). In addition, sensor nodes have limited storage and computational resources, rendering public key cryptography impractical.

The medium in which the MANET operates on is air, so it is more vulnerable to various types of attack. In MANET the nodes communication with each other on the basis of their unique identity which is mapped in form of one to one mapping in between an identity and an entity. Various protocols are there to form an Ad-hoc network among the mobile and radio equipped devices. There is an attack called Sybil attack , Which fails the security applied by various protocol. An example , of Sybil attack, where their must be assurance that each identity is actually one entity. This assurance requires costly manual intervention by which we can restrict the number of identities.

To ensure secure communication it is necessary that we should eliminate the malicious node from our network. In this paper, we show that the mobility can only be used for the detection or to identify the malicious nodes. We can also use various algorithm, but the algorithm must satisfy on these points first:

- Authenticity: It means the trueness and validness of the node participating in the communication.
- Availability: All nodes and their service must present all the time.
- Confidentiality: Authorize access must be their for the user.
- Non-repudiation: Sender and Receiver can't deny that they have send the message.

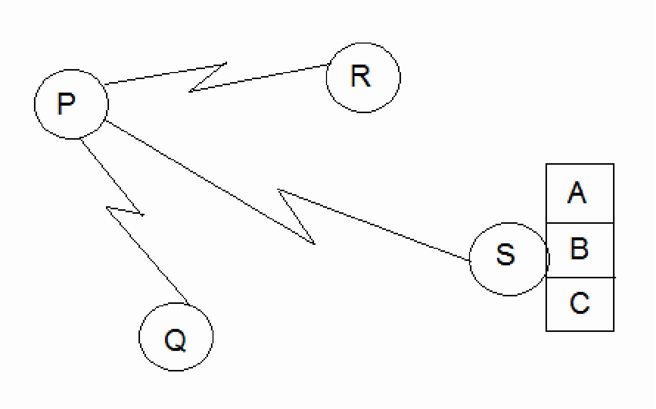

Fig. 2 – Sybil attacker with multiple identities

In this figure the node S is a malicious node with multiple identities A,B,C, When a node communicate with S then it will have an illusion like it has communicated with 4 other node while it is the single. In actual it is the one node which have multiple ID's.

The two method to identify are

- Passive Ad-hoc Sybil attack detection which is based on MAC address.
- PASID with Group detection, in which we will see the false identity or the node with multiple ID's are more dense.

II. Related Work

Related Work The Sybil attack was first described by Douceur in the context of peer-to-peer networks [6]. He pointed out that it could defeat the redundancy mechanisms of distributed storage systems. Karlof and Wagner noted that the Sybil attack also poses a threat to routing mechanisms in sensor networks. J. Newsome et al. proposed a solution for detect on through radio resource testing and randomly pre key distribution. They present an excellent discussion of threat that Sybil attack poses to sensor network, all of which apply to MANET. The work was on wireless sensor network where we require the active participation of the neighbor node to identify the identity, which is difficult to implement in MANET or there are changing nodes in its environment.

Generally Sybil attack occurs in distributed systems which does not have any central authorities because here each entity is only aware of other through message over the channel. An entity can determine the set of entities are distinct by testing resources limits, but this is problematic. If a single Sybil attacker pretends to be multiple entities, it may not have the same computational, storage and bandwidth capabilities as multiple independent identities.

This paper makes the following contributions. We introduce a taxonomy of the different forms of the Sybil attack as it applies to wireless sensor networks. We analyze how an attacker can use the different types of the Sybil attack to perturb or compromise several sensor network protocols. Douceur was the first to introduce the Sybil attack, Douceur has shown that a Sybil attacker can not be prevented by test of finite resources. Douceur also suggested that there is no practical solution for Sybil attack. For eliminating it completely, Trusted certification is the only scheme. But it too suffer from costly initial set up and a single point of failure.

III SYBIL ATTACK TAXONOMY

We define the Sybil attack as a malicious device illegitimately taking on multiple identities. We refer to a malicious device's additional identities as Sybil nodes. To better understand the implications of the Sybil attack and how to defend against it, we develop a taxonomy of its different forms.

forms. We propose three orthogonal dimensions: direct vs indirect communication, fabricated vs stolen identities, and simultaneity.

3.1 Dimension I: Direct vs. Indirect Communication

Direct Communication One way to perform the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Likewise, messages sent from Sybil nodes are actually sent from one of the malicious devices.

Indirect Communication In this version of the attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed through one of these malicious nodes, which pretends to pass on the message to a Sybil node.

3.2 Dimension II: Fabricated vs. Stolen Identities

Fabricated Identities In some cases, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value.

Stolen Identities Given a mechanism to identify legitimate node identities, an attacker cannot fabricate new identities. For example, suppose the name space is intentionally limited to prevent attackers from inserting new identities. In this case, the attacker needs to assign other legitimate identities to Sybil nodes. This identity theft may go undetected if the attacker destroys or temporarily disables the impersonated nodes.

3.3 Dimension III: Simultaneity

Simultaneous The attacker may try to have his Sybil identities all participate in the network at once. While a particular hardware entity can only act as one identity at a time, it can cycle through these identities to make it appear that they are all present simultaneously.

Sohail Abbas el at. [8] proposed a n RSS-based detection mechanism. This work by using IEEE 802.11 standard on MAC layer, without any hardware.

P. Kavitha el at. [9] proposed a detection technique using NDD algorithm. In this the algorithm is used to transfer data from source to destination without any loss. Address are stored by the neighbor and which ensure the correct destination.

Roopali et al. [10] propose a technique in which all three parameters are checked when node enters a network, the parameters are speed, energy and frequency and if value of all these parameters are less than threshold value then node is considered as legitimate node otherwise as Sybil node.

Yamini D.Malkhed el at. [11] Proposed a detection technique which is based on RSS along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive. By Authentication means only legitimate nods are allowed to come in to the network. As well as Lower-bound detection threshold is used, and compare with Received Signal

Strength (RSS) value, if the comparison is greater than or equal to RSS value, then it’s a Sybil identity (Whitewash identity). Otherwise it’s a legitimate node in the network.

Sybil attacker wishes to keep their multiple identity same as the system. There is a difference between the legitimate node and a Sybil attacker , in General the independence node are mobile but that of Sybil node the identity move together and this provide a way to find Sybil attack in a network.

IV ATTACKS

In this section, we examine how the Sybil attack can be used to attack several types of protocols in wireless sensor networks.

4.1 Known Attacks

Distributed Storage Douceur observes that the Sybil attack can defeat replication and fragmentation mechanisms in peer-to-peer storage systems [6]. The same problem exists for distributed storage in wireless sensor networks.

Routing Karlof and Wagner point out that the Sybil attack can be used against routing algorithms in sensor networks [9]. One vulnerable mechanism is multipath or dispersity routing where seemingly disjoint paths could in fact go through a single malicious node presenting several Sybil identities.

4.2 New Attacks

Data Aggregation Efficient query protocols [13] compute aggregates of sensor readings within the network in order to conserve energy rather than returning individual sensor readings. A small number of malicious nodes reporting incorrect sensor readings might be unable to significantly affect the computed aggregate.

Voting Wireless sensor networks could use voting for a number of tasks. The Sybil attack could be used to “stuff the ballot box” in any such vote. Depending on the number of identities the attacker owns, he may be able to determine the outcome of any vote.

Fair Resource Allocation Some network resources may be allocated on a per node basis. For example, nearby nodes sharing a single radio channel might each be assigned a fraction of time per interval during which they are permitted to transmit.

V. PRPOSED DETECTION TECHNIQUE

Sybil attacker establishes the identity by IP address, MAC address or public key, these differ from the real node in several ways. As the resources of single node is used to simulate multiple identities. Douceur has proposed that it is difficult to prevent from the test of finite resources. The Sybil attacker must share the same set of resources unlike the other entities.

In our proposed solution any node can start the detection for the Sybil node.

In our simulation the node which will cat as detecting node will be the sender, when the sender wants to sned a message “HELLO”, before sending this message this message the sender wants will broadcast request message and will wait for the reply message. Sender will compare the logical address that is IP and physical address that is MAC. Here the sender will observe those node which are having the same MAC address but the reply is different in form of IP address. Everything the logical address is changed over the MAC address, and these types of nodes are declared to be the Sybil node

A. Following are the steps which involves in the detection:

- Sender Broadcast the request message.
- Message received by all nodes present in MANET.
- Sender receives the reply message containing MAC and IP address.
- Comparison of MAC address from all nodes.
- If two IP having same MAC address then Sybil node and find another route to send message.
- Else otherwise accept the packet and send.
- Exit.

The flow chart diagram for the detection of the Sybil attack in the MANET is shown below which will show the flow of the message in the nodes ,when the sender sends the message it will generate a request message before it and will broadcast the message, the sender will wait for the reply message and when it get the message will inquiry on its aspects of IP and MAC address and thus identify the malicious node in the network.

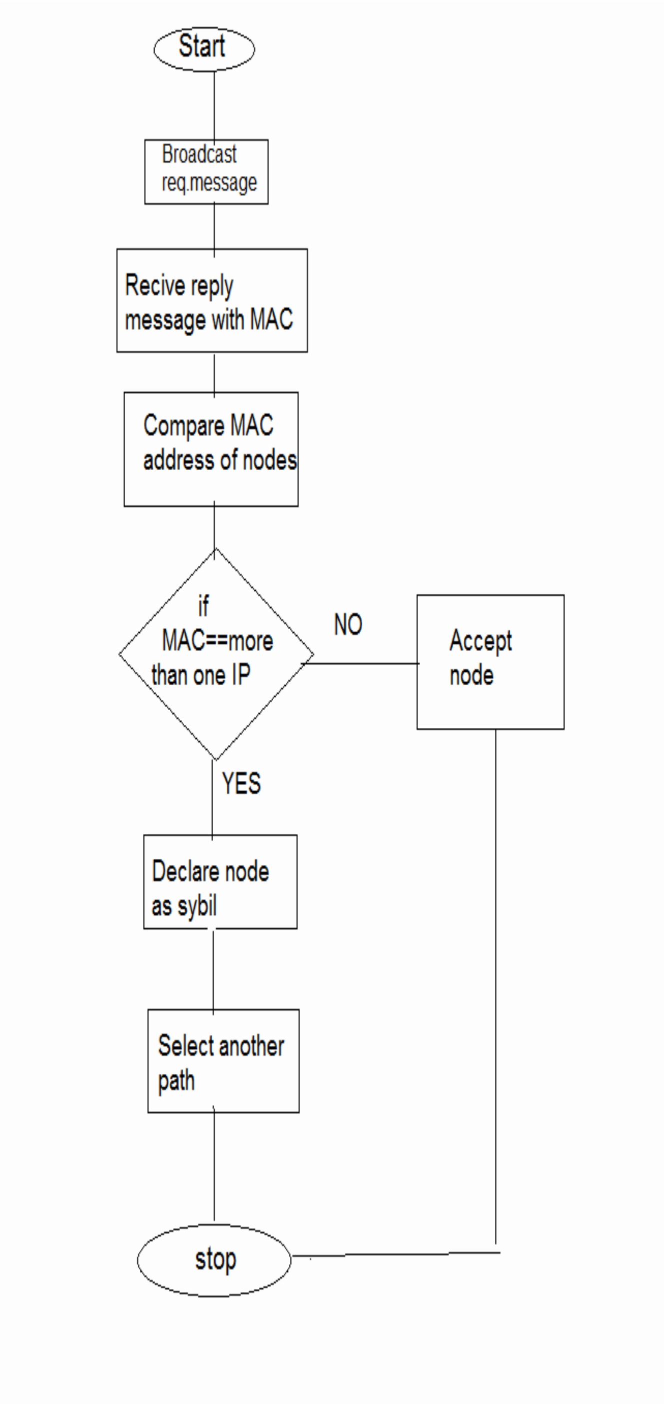

Fig 3: Architecture for detection and prevention of Sybil node

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[7] Electronic Publication: Digital Object Identifiers (DOIs): Article in a journal:

[8] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.
Article in a conference proceedings:

[9] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

[10] M. Ramkumar, N. Memon, KPI: A Security Infrastructure for Trusted Devices, Pre-Conference.

[11] M. Mohammed, "Energy Efficient Location Aided Routing Protocol for Wireless MANETs", International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2, 2009

[12] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010.