International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 6, Volume 2 (June 2015) www.ijirae.com

ARCHITECTURE FOR DETECTION OF SYBIL ATTACK IN MANET USING MAC ADDRESS

Anamika Pareek
M.Tech(CSE)
Sanghvi Institute of Management & Science, Indore

Mayank Sharma
Sr.Lecturer (CSE)
Sanghvi Institute of Management & Science ,Indore

Abstract—Ad hoc network is improved method of communication which reduces the network overhead and also opens a wide spectrum for attacker to break the security. As wireless communication happens through open air, it also increases possibility of fetching the information from air medium using sniffing software tools. A particularly harmful attack against Mobile Ad hoc network is known as the Sybil attack. When an attacker intrudes in the network and acts with multiple identities to disrupt the normal and trustworthy communication between nodes. In this paper we presented an architecture for detecting the sybil attack using Mac Address . Analysis have found some solution that include the communication among the nodes of cluster and analyze the results in different scenarios like fake sender detection, fake receiver blocking, node to node secure connection and packet acceptance and rejection process

Keywords— MANET, Sybil attack, fakes Identity, Multiple Identities, vulnerable.

I. INTRODUCTION

Ad hoc networks is a wireless network that consist of number of mobile nodes that are connected by wireless links, these nodes uses radio frequency channel as their physical medium for communication .An ad hoc wireless network are defined as the category of wireless network that utilize multi hop radio relaying and are capable of operating without the support of any infrastructure ,hence they are also known as Infrastructure less network. Those nodes that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Ad hoc networks can be used for battlefield emergency, law enforcement, and rescue missions.

In MANET nodes communicate with each other on the basis of unique identity that forms the 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 represents two different nodes. But the malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping of identity and entity philosophy. Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Like this, it disturbs the communication among the nodes of the network.

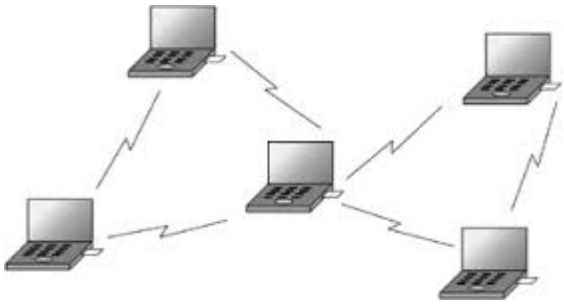

Fig 1: Ad hoc Network

To have secure communication it is necessary to eliminate the Sybil nodes from the network [1]. The following goals must be fulfilled by security algorithm used to detect the attack [2]:

- Authentication: It means that each and every node, participating in communication must be genuine and legitimate node.
- Availability: All services should be available all the time to all the nodes for the proper functioning and security of the network.
- Integrity: It gives the assurance that the data received by the receiver will be same as the data send by the sender.
- Confidentiality: It means that some data is only accessible by the authorized users.
- Non-repudiation: It means sender and receiver cannot deny that they didn't send or receive the data

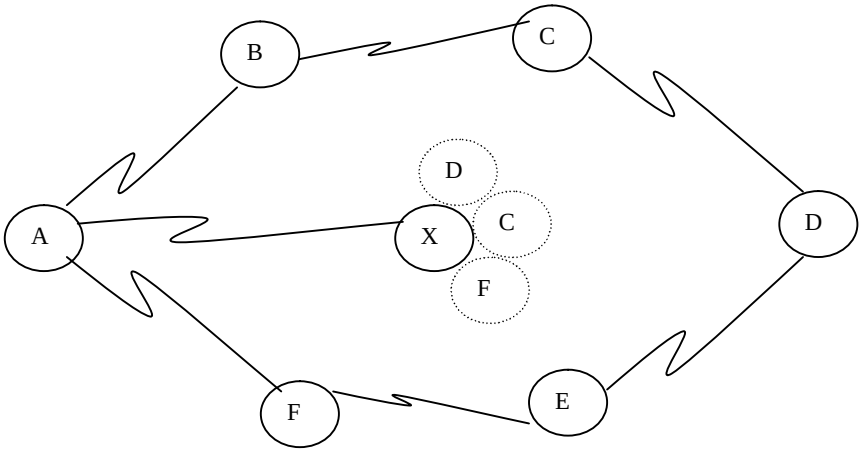

Fig 2: Sybil Attacker with multiple Identities

Figure 2 represents a malicious node X along with its three Sybil nodes (C,D and F). If this malicious node communicates with any legitimate node by presenting all its identities, the legitimate node will have illusion that it has communicated with four different nodes. But in actual, there exists only one physical node with multiple IDs.
This paper is organized as follows:
In Section 2 we present different detection techniques for Sybil attack. Section 3 presents summary of these techniques and Section 4 shows Conclusion

II SYBIL ATTACK

Sybil attack was first introduced by Douceur [2].According to the Douceur a malicious node can generate and control a large number of logical identities which gives illusion that there are number of different identities are present but in actual only one physical node is present. Douceur showed that there is no practical solution for this attack. Deploying Trusted Certification is the only scheme that can completely eliminate the Sybil attack. However, it suffers from costly initial setup, lack of scalability and a single point of attack or failure. Also, it's based on the assumption that each entity has single identity which is very difficult to achieve on the large network.

A *Types of Sybil Attack:*

There are different types of Sybil attack as mentioned below [13]:
1) Direct and Indirect Communication: In direct communication the communication is between the legal node and the Sybil node while in indirect communication it is between the legal node and the copy of the Sybil node.
2) Stolen and Fabricated Identities: Stolen identity is that identity which the malicious node takes from the legitimate node and uses of attack. This kind of cannot be identified and find if the legitimate node is destroyed. While fabricated identities are that identities that the copy node or the malicious node takes from the legitimate node or we can say uses the exact same identity as that of the legitimate node. This is known as identity replication in which same identity is used many times in a same network
3) Simultaneous and Non Simultaneous Attack: In simultaneous attack, all the copy nodes or the Sybil identities participate at the same time, but since they have only one identity so this simultaneous attack is supported by the cycling of identities between all nodes. Non simultaneous is that in which the attacker uses the same number of the identities equal to number of devices.

III DETECTION TECHNIQUES

A Trusted Certification

Trusted certification is the most common solution, mainly due to its potential to completely eliminate Sybil attacks Douceur et al [2]. However, trusted certification relies on a centralized authority that must provide guarantees that each node is assigned exactly one identity, as indicated by possession of a certificate. In fact, [2] offers no method for ensuring such uniqueness, and in practice, it has to be performed by a manual configuration. This manual procedure can be costly, and create a performance bottleneck in large-scale systems. Additionally and in order to be effective, the certifying authority must guarantee the existence of a mechanism to detect and revoke lost or stolen identities. These requirements make trusted certification very difficult to implement in ad hoc networks, which lack, by definition, a centralized authority that can provide the certification service.

B Trusted Devices

The use of trusted devices can be combined with trusted certification, binding one hardware device to one network entity. While this can effectively mitigate the Sybil attack, the main issue with this approach is that there is no efficient way to prevent one entity from obtaining multiple hardware devices other than manual intervention Martucci et al. [3].

C Domain Specific

There are some countermeasures that are application-domain specific. For example, in Piro et al [4], a detection mechanism for mobile ad hoc networks is proposed, based on the location of each node. For an attacker with a single device, all Sybil identities will always appear to move together. However, the defense is not applicable beyond mobile networks.

D Resource Testing

The main goal of resource testing is to attempt to determine if a number of identities possess fewer aggregated resources than would be expected if they were independent. In resource testing, it is assumed that each physical entity has a limited amount of a given resource (e.g., limited bandwidth). The verifier then tests whether identities correspond to different physical entities by verifying that each identity has as much resources as an independent physical device should have. These tests include checks for computing power, storage ability and network bandwidth [2]. A type of resource test is employed by the Sybil Guard technique Yu et al [5] which relies on the limited availability of real-world friendship edges between nodes.

E Received Signal Strength based Detection:

Roopali et al. [6] proposed the use of Received Signal Strength to detect Sybil attack. In proposed technique when node enters a network, then it's all three parameters are checked i.e. 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 .Nidhi et al.[7] proposed the RSS based detection approach along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive. For the authentication of node, Message Authentication Code (MAC) is used. Authentication of node allows only legitimate node to come in to the network. As well as Lower-bound detection threshold is used, and compare with Received Signal Strength (RSS) value.

F Recurring Costs and Fees

There are several works in the literature that describe mechanisms in which identities are periodically re-validated using resource tests Maniatis et al.[8]; Maniatis et al.[9]. This technique is a variation of the normal resource testing, and can limit the number of Sybil nodes an attacker, with constrained resources, can introduce in a period of time. Recently, it was shown Boris & Levine et al [10], that charging a recurring fee for each participating identity is more effective as a disincentive against Sybil attacks. For many applications, recurring fees can incur a cost to the Sybil attack that increases with the total number of identities participating; whereas one-time fees incur only a constant cost.

G Hash Function Based Detection

Danish Shehzad el at. [11] Proposed a detection technique based on Hash Function, only messages along with their hash function are accepted each individual node detects Sybil attackers by validating the Hash received along with message by neighbor, after receiving message node gets Hash of sender and compares it with the previous Hash received in Hello message for the validation of its identity. If Identity or Hash differs to that of Hash received along with hello message than node is nominated as Sybil and node is blocked from any communication.

H Random Key Predistribution

This technique enables nodes on a wireless sensor network to establish secure links for communicating with each other [12]. In random key predistribution, a set of keys are assigned at random to a node enabling it to discover or compute the common keys that it shares with its neighboring nodes. Node-to-node secrecy is ensured by using the common keys as a shared secret session key. The main ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation involves ensuring that the network is able to validate the keys that an identity might have. The forged Sybil identity will not pass the key validation test as the keys associated with a random identity will most likely, not have an appreciable intersection with the compromised key set.

IV PROPOSED ARCHITECTURE

In the proposed Architecture for detection of Sybil attack, any node can start the detection for Sybil node. In our case sender node starts detection for Sybil node before it sends packets to the receiver node. Firstly sender node broadcast a request packet which in return wants a reply message which contain logical (IP) address and physical address (MAC).sender nodes maintain a table for that and checks if a node with same physical address reply with different logical address then the node with different logical identity is declared as a Sybil node and the sender node chooses another path for sending packets to destination.

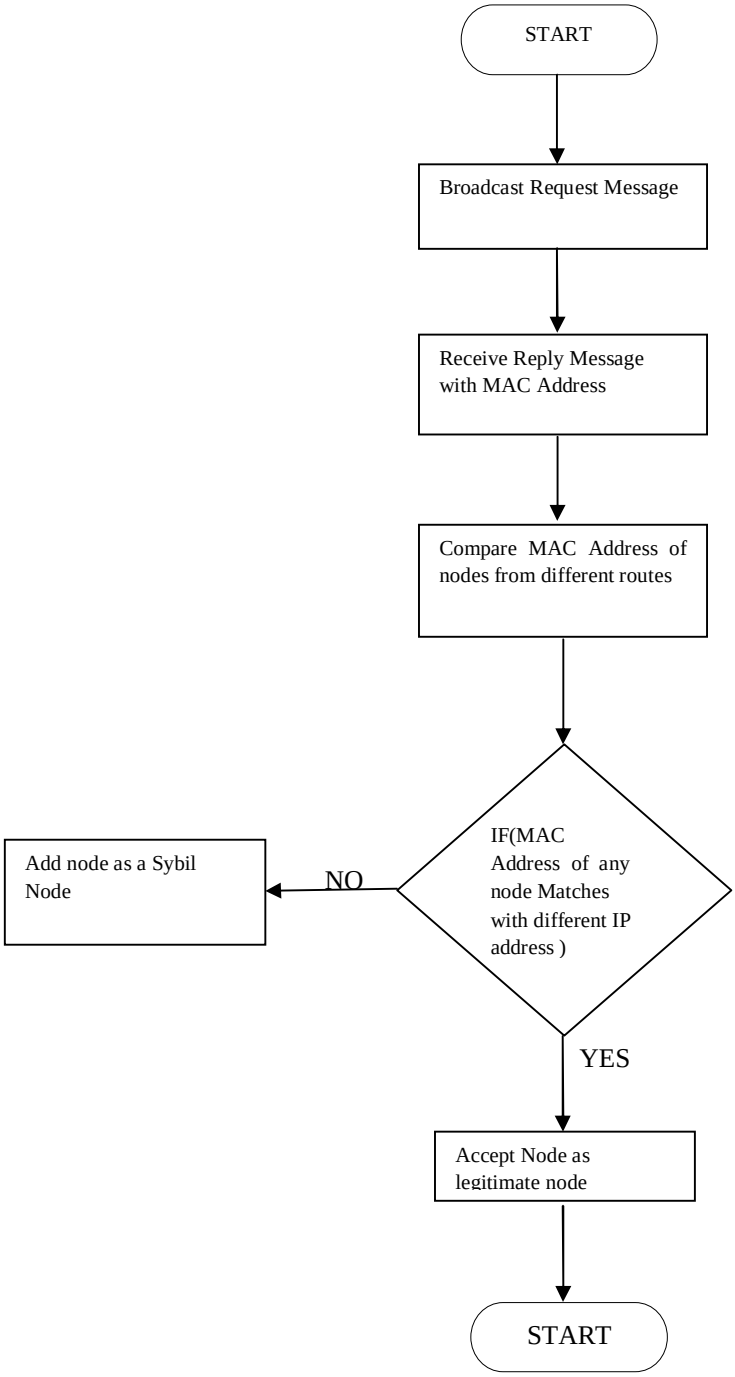

Fig 3: Architecture for detection of Sybil node

IV CONCLUSION AND FUTURE WORK

MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe Communication it is must be secure network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, it uses multiple identities or uses the identity of another node present in the network to disrupt the communication or reduce the trust of legitimate nodes in the network. In this paper we have given Architecture to detect Sybil nodes to safeguard the network. In future the proposed architecture is implemented and tested in network

ACKNOWLEDGEMENT

We wish to thank the editors and reviewers for their valuable comments. We are thankful to our professors for being the best guide and advisor for this research work in every field we have taken to complete our requirement.

REFRENCES

[1]Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, pp.1-19, 2012.

[2]J. R. Douceur,"The Sybil Attack," presented at the Revised Papers from the first Int. Workshop on Peer-to-Peer Systems, pp.251-260,2002

[3]Martucci, L., M. Kohlweiss, C. Andersson, & A. Panchenko . Self-certified sybil-freepseudonyms. In WiSec '08: Proceedings of the first ACM conference on Wireless networksecurity, New York, NY, USA, pp. 154–159. ACM.2008

[4]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

[5]Yu, H., M. Kaminsky, P. Gibbons, & A. Flaxman . Sybilguard: Defending against sybil attacks via social networks. Networking, IEEE/ACM Transactions on 16 (3), 576–589 2008.

[6]Roopali Garg, Himika Sharma "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 5, May 2014

[7] Nidhi Joshi,Prof Manoj Challa,"Secure Authentication Protocol to Detect Sybil Attacks in MANETs" International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 06 Jun 2014

[8]Maniatis, P., D. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, & Y. Muliadi . Preserving peer replicas by rate-limited sampled voting. SIGOPS Oper. Syst. Rev. 37 (5), 44–59.2003

[9]Maniatis, P., M. Roussopoulos, T. Giuli, D. Rosenthal, & M. Baker . The lockss peerto peer digital preservation system. ACM Trans. Comput. Syst. 23 (1), 2–50 2005.

[10]Boris, N. M. & B. Levine . Quantifying resistance to the sybil attack. In Proc. Financial Cryptography (FC)2008..

[11] Danish Shehzad, Dr. Arif Iqbal Umar, Noor Ul Amin, and WaqarIshaq " A Novel Mechanism for Detection of Sybil Attack in

MANETs" International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UA)

[12] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. *In ACM CCS 2003*, pages 42–51, Oct. 2003

[13] J. Newsome, E. Shi, and D. Song, "The Sybil Attack in Sensor Network: Analysis & Defenses," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: CAN Press, 2004, pp.185-191.

