IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.685-690, ISSN: 2347–8586

AN EFFICIENT METHOD TO DETECT AND PREVENT SYBIL ATTACK

Balamalathy.N
PG Scholar, Department of Computer Science,
S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, India.
malathyrj@gmail.com

Parvathi.S
Assistant Professor, Department of Computer Science,
S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, India.
5680sparvathi@gmail.com

Kumaresan.A
Phd scholar, Computer Science and Engineering, SKP Engineering College
,Thiruvannamalai, Tamil Nadu, India.

Abstract- In adhoc network is the major problem for providing security in the network. For servers, there is no infrastructure A network connection established for a single session and cannot require a router or a wireless base station in computer networking. An adhoc network is created for a specific purpose and adhoc network is a temporary network connection (such as data transferring from one node to another). It is used to without loss of data and to enhance security. Sybil attack, in which an attacker manages and control to more than one identity on a single device. It is strongly desirable to detect and prevent a Sybil attack and eliminate them from the network. In this paper, Sybil attack can detect and prevent from the attackers. It can detect and prevent the information from sender to receiver without loss of information using Neighbor discover distance (NDD) algorithm. An NDD algorithm detects neighbor node and act as a server to send information to destination. In this method passive adhoc identity method and key distribution are used. Detection can be done by a single node or multiple nodes can join to improve the accuracy of detection. It can be used to secure and avoid attacking the system on the network.

Index Terms: *Sybil attack, Neighbor discovers the distance (NDD), adhoc network*

I INTRODUCTION

Adhoc networks represent distributed systems. Adhoc network consist of wireless mobile nodes that can freely self-organize into arbitrary and temporary. The unique characteristics of Adhoc networks, such as dynamic topology and constraint devices, number of nontrivial challenges for efficient and lightweight security protocols. A Centralized identity management in Adhoc network and requirement of a unique, distinct, and persistent identity for their security protocols. A Sybil attacker can damage to the Mobile adhoc networks in several ways. For example, an attacker can disrupt multipath routing or location-based by participating in the routing, giving the false impression of being distinct nodes at different node-disjoint paths. At the same time attacker can use the different identities. A single attacker could pretend nodes to report the existence of a false bottleneck in traffic. Adhoc network is mainly used to gather sensitive information about mobile nodes. To relate between a source and its destination, effect on data and transmission time on the network. A end-to-end network is a piece of software. It can access only local resources. An entity on the end-to-end network by presenting an identity. A more than one entity can correspond to a single entity. Basically, the mapping of identities to entities is many to one. In this type of networks use multiple identities, Such as redundancy, resource sharing and integrity. Adhoc network is the evolving wireless communications. Self organized ad hoc networks by PDAs or laptops. Its use in conference, disaster relief and battlefield environments. The traditional problems of adhoc network are power control, transmission-quality enhancement.

SYBIL ATTACK

Sybil attack uses a single node in several invented addresses. Our technique allows detecting malicious and Sybil nodes within ADHOC by using received signal strength variations, localization verification and nodes distinguish ability degree evaluation. Distributed work systems arise in many places, for example P2P file-sharing networks or wireless ad hoc networks. An individual peer route data packages for each other. The total amount of work consumed by a population is equal to the total amount of work performed. Security mechanisms are basis of vulnerable and exact assumptions of identity to attack, when these presumptions are wrong. The next type of identity certificates is shared by multiple users. The Sybil attack is a targeting reputation system, including real-world systems. Example eBay. A proposes system model against such as a system in a certain division of the nodes are honest. This attack can control the trusted central authority. That authority provides issues and verifies recommendation unique to normal users. Sybil attack is solving more difficult and challenging problem. In malicious user creates a number of peer identities know as *sybils*. Sybil attack is a major attack where a single node has multiple identities. When a Sybil node act as a sender, it can send false data to its neighbors. When it acts as receiver, it can receive the data which is originally destined for a legitimate node.

II RELATED WORKS

The Sybil attack was described by Douceur in the context of P2P networks. He mainly pointed out that it could more damage the redundancy mechanisms of storage distributed systems. In such situations, Douceur has shown this attack cannot prevent. A effects of the sybil attack considered the different variety of applications. Karlof and Wagner best distinguished that the Sybil attack poses a more risk to routing systems in sensor. Piro et al. [7] Proposed a scheme to detect the Sybil nodes by examining the behavior of nodes. According to this scheme, the nodes which move freely, independently in different directions are considered as legitimate nodes and the nodes which moves together are suspected as Sybil nodes and it keeps observing these suspected nodes. This scheme gives high false positive results when group of nodes moves in the same direction. In [7] [11] two approaches are discussed to detect the Sybil attacks. First is proactive approach which includes economic incentives [12] [10] and pre key distribution [4] [14] techniques. Second is reactive approach which is based on testing of resources and location of nodes. J. Newsome et al. [8] Proposed a scheme in which radio resource testing and randomly pre key distribution are done to detect the Sybil nodes. In [5] [6] authors proposed DCA scheme. In this scheme, certificates are distributed to all nodes present in the network and nodes use these certificates as a proof of their identities. It helps to prevent the Sybil attacks. Athichart Tang pong et al. [9] proposed a technique known as Robust Sybil attack detection technique. In this technique the behavior of the nodes is examined. The nodes having the similar path are detected as the Sybil nodes. Hongbo Zhou [13] proposed a secure prophet address allocation scheme. In this scheme unique address is distributed to all nodes present in the network. If some new node enters a network, then unique address is provided for that node which does not match with address of any node present in the network. This helps to prevent the Sybil attack.

III EXISTING SYSTEM

In the existing system, the source node sends a message to the destination node, but hackers can act as source nodes to send message to the destination node. So that destination receives a message from the hacker, but it wasn't the wrong message. Destination trust that its correct message from the sender. On the other hand, destination receives the wrong message from hackers. In loss of security, sender passes messages to receivers. This attack poses a serious threat to such sensor networks. An single physical device attacker can create more than one identity in launch a coordinated attack on the network or switch identities weaken the detection process. In the network promoting lack of accountability. The source node maintains Header information to pass the data to a receiver. Hackers can easily modify that header information, so more data can loss and damaged.

The disadvantage is destination receives the inaccurate information from hackers or malicious node, there is any other server cannot detect hackers, it leads to loss of data and network performance is low.

IV PROPOSED SYSTEM

In this proposed system, hackers cannot act as a sender, as one centralized server is maintaining to check the authentication of the source. It blocks unauthorized users or hackers. To provide a key based data transmission and id based network. Passive adhoc identity like as Neighbor discover distance (NDD) node to watch the transmission on the network. Our proposed system used the NDD Algorithm. Use these algorithms to transfer the data from 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 into the correct destination. If they have any data loss and damage are some collision on the network. It immediately to inform the server to stop the packets transfer and maintaining sender node and header information.A users check the those details whether they are attackers or actual user. Hacker's information has cannot change or modify data to the destination. The receiver has not been receiving any attacker information. In our proposed method to use, secure and avoid the attacking system on the network. The benefits are to reduce the packet delay and detect the attacker, data delivery quickly from source to destination. Efficient data transmissions on the network, Without any loss data will be sent in destination and improve the network performance and also prevent data. In our proposed scheme work to detect and prevent data from peer to peer network.

DETECTION IN SYBIL IDENTITIES

The two different types of Sybil attacks. An attacker creates identity while previously created identity can reject it; its also know as whitewashing attack or join-and-leave and the stimulus is to delete bad history of malicious activities. In the next type of attack, all its identities concurrently use to an attacker, know as a simultaneous Sybil attack. The stimulus of this attack is to cause gain more resources or rupture in the network, etc. Than that of a one node deserves in a network.

The attacker joins the network with its single identity, and malicious nodes cannot collude with one another node. The attackers can get two different way of identities,such as

1. Fabricate identities
2. Stolen identities

A. RSS ALGORITHM BY USING SYBIL ATTACK FOR DETECTING

The neighborhood joining behavior can be based on their a legitimate node and Sybil identity. When the attacker can create a new Sybil identity means automatically signal strength will be higher. To distinction between a new node and a Sybil identity in entrance behavior.

ALGORITHM 1

addRss (***Addr1***, ***rss1***, ***recv_time***)
BEGIN SUB:
IF: Address is not presented in the Table1
THEN:
IF: rss1 >= UB−THRESHOLD
THEN: Add to Malicious codelist (Addr1)
Basecast Detect Update(Addr1)
ELSE: Add to Table1(Addr1)
END IF
Create Record(Addr1)
Push_back(rss1,recv_time)
IF: list_Size > LIST_SIZE
THEN: Pop_front()
END SUB:

ALGORITHM 2

```
IF: RSS1 TIMEOUT
THEN: rss1Table1Check( )
Rss1Table1Check()
BEGIN SUB:
FOR: for each Addr1 in the Table1
DO:
Pop element()
IF: (Current Time_getTime ()) >
TIME−THRESHOLD
From this Addr1 since the TIME_
THRESHOLD
THEN:
IF: getRss1() > UB_THRESHOLD
THEN: Add to Malicious code List
(Addr1)
Whitewasher
ELSE:
END FOR:
END SUB:
```

PREVENTION IN SYBIL IDENTITIES

Validation techniques can be benefited to prevent for Sybil attacks and discard masquerading inimical entities. A remote id may accepted by a local id depend on a central authorization which make a secure a one-to-one concurrence between an entity and an identity and may even produce a search for revoke. In this technique are validated techniques fully depend on an identity either indirectly or directly

1.. In direct validation to validate the remote identities to local entity inquiries the central authorization.
2. In indirect validation the entity only depends on approved identities which in turn endorse for remote identity.

B.NEIGHBOR DISCOVERS DISTANCE (NDD) ALGORITHM BY USING SYBIL ATTACK FOR PREVENTING

Neighbor Discover Distance algorithm used to detect the sybil attacters. In Manet each and every nodes consists of a neighbors data address.The neighbors data address transfer to destination without any packet loss. NDD algorithm is more security and efficient data transmission on their network.

ALGORITHM

Step 1: The neighbor node address to know every node .

Step 2: If neighbor node is known as centralized server node, that node Store the data Or search the centralized node.

Step 3: The server nodes maintain all source and destination data address.

Step 4: Each node have the individual keys. Each individual key depends on the centralized server is to identify the destination data address.

Step 5: In Neighbor discovers distance algorithm and centralized server method is mainly used for preventing the data into any attackers/hacker

Step 6: check whether a destination node address is correct or not.

Step 7: If any data is damage means destinations node sending the data in a centralized server.

V IMPLEMENTATION

OBJECTIVE

i) Using NDD algorithm based to find detection and prevention sybil attack.
ii) To use, secure and avoid the attacking system on the network.

The above concept is implemented with the following technology framework.First, server setup method for node creation. In the server setup process the admin first sets the remote servers IP-address for sending that IP-address of the receiver. The Server may check process is either an active or deactive process. Active process is the nodes are registered in the server. So, it shows an available address in the server. So it shows an available address in the server. The activated IP-address are stored in available storage servers.Deactive process is nodes are not registered in the server. So it cannot show available IP-address in the server. The currently available IP-address can be viewed, Others it can be deactive process to be detection of sybil attack.The client sends a message to receivers without loss of data using key distribution. The Key distribution and passive adhoc identity for prevention of sybil attack. The Server sends a message to clients using auto-generate code to receive messages. The Message is secure and without loss of data. Servers send a header message to the receiver using NDD algorithm, file transmission on secure process.

OVERVIEW

Server register number of nodes/clients. Those register nodes are active others deactive processed. The Server sends a message to the client using key distribution and also auto-generate code to nodes. The key distribution and passive adhoc identity for detection and prevention of sybil attack. Using NDD algorithm, message receive without loss of data and file transmission on secure process.

VI RESULT

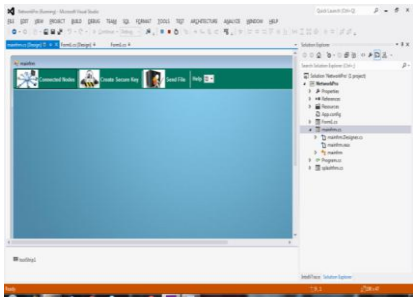

Fig 1 : oview of the model

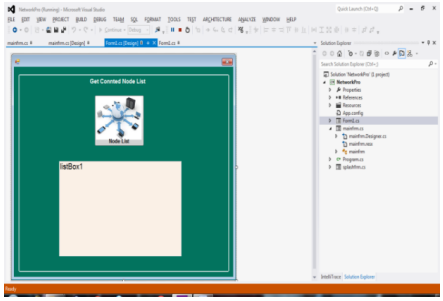

Fig 2: Nodes transmission

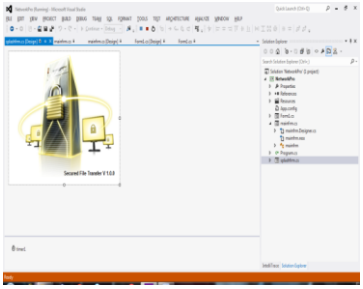

Fig 3: Secure nodes from attacker

VII Conclusion

The proposed NDD algorithm-based detection mechanism to Sybil attacks. Use these algorithms to transfer the data from 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 into the correct destination. The many influences affecting the accuracy of detection, such as network, data transmission rates, various node density and speed rate. To detect both join-and-leave and simultaneous Sybil attackers consist of high degree of accuracy, Our scheme works showed the simulation results. In future method to use, secure and avoid the attacking system on the network.

REFERENCES

[1] Sohail Abbas, MSdjid. David Llewellyn-jones, and Kashif kifayat, " Lightweight Sybil Attack Detection in MANETs", IEEE SYSTEM JOURNAL, VOL.7,NO.2,JUNE 2013.

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

[3] 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.

[4] N. B. Margolin and B. N. Levine. Quantifying sybil attacks againstnetwork applications. Technical Report 67, Dept. of Com. Sci., U. MassAmherst, Dec. 2005.

[5] SaroshHashmi, John Brooke,``Towards Sybil Resistant Authentication in Mobile Ad-hoc Networks "FourthInternational Conference on Emerging Security Information,System and Technologies, pp.17-24, 2010.

[6] SaroshHashmi, John Brooke,``Authentication Mechanisms for Mobile Ad-hoc Networks and Resistance to Sybil Attack " The Second International Conference on Emerging Security Information,System and Technologies, pp.120-126, 2008.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis &defenses," in Proceedings of the third international symposium on Information processing in sensor networks. Berkeley, California, USA: ACM, 2004.

[8] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in ProcSecurecomm Workshops, pp.1–11,2006.

[9] HongboZhuo,``Secure Prophet Address Allocation for Mobile Ad-hoc Networks" IFIP International Conference on Network and Parallel Computing, pp.60-67, 2008.

[10] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. La Porta.Establishing pair-wise keys in heterogeneous sensor networks. In Proc. IEEE INFOCOM,Apr, 2006

[11] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks : Analysis &defenses. In Proc. IPSN'04, Berkeley, Apr. 2004.

[12] N. Margolin and B. Levine. Informant: Detecting sybils using incentives.Financial Cryptography, Feb. 2007.

[13] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning.Defending against Sybil attacks in sensor networks.In Proc. IEEE ICDCS, June 2005

[14] AthichartTangpong, George Kesidis, Hung-yuanHsu,AliHurson,``Robust Sybil Detection for MANETs " IEEE, 2009

[15] Jin-HeeCho,AnanthramSwami,andIng-Ray Chen,``A Survey on Trust Management for Mobile Ad Hoc Networks for Mobile Ad-Hoc Networks," IEEE Communication Surveys & Tutorials, Vol.13, No.4, pp.562-583, 2011.