ISSN 2277-3061

Prevention Techniques for Sybil Attack

Roopali Garg, Himika Sharma
Co-ordinator,deptt of IT,UIET, Panjab University, Chandigarh
roopali.garg@gmail.com
Research Scholar,deptt of IT,UIET, Panjab University, Chandigarh
himikasharma3@gmail.com

ABSTRACT

Mobile ad-hoc network is a self-governing network, consists of group of nodes that communicates with each other through wireless links. As it is a wireless network, so it is subjected to various attacks. There is one attack which is very dangerous called Sybil attack. In Sybil attack, attackers or malicious nodes uses multiple identities to disrupt the communication between the nodes by capturing necessary and important information and creating misunderstandings between the nodes. In this paper some measures are described to prevent Sybil attack.

Keywords

MANET-Mobile ad-hoc network; RSS-Received Signal Strength; MC-DCA-Multiple Key Cryptography based on Distributed Certificate Authorities.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 11, No.10
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 2277-3061

INTRODUCTION [1][2]

MANET is a self-governing network, consists of group of nodes that communicates with each other through wireless links. When node enters a network then it requires unique address to communicate with other nodes present in the network. As MANET is a decentralized network, so there is no authority in the network which verifies the identities of the nodes. Sometimes there are attackers who misuse this property of MANET. In this attacker uses identity of another node or some other identity to create misunderstandings between the communications of nodes present in the network or to collect some important information. This type of attacks is called Sybil attack. Sybil word itself explains the Sybil attack which means multiple identities and it is named after the famous multiple disorder patient whose name is “Sybil”(Shirley Ardell Mason). A Sybil attacker can create a lot of damage or destruction to the network in many ways like reduce the trust of the nodes by sending fake information about that node in the whole network and also create misunderstandings among the nodes by not forwarding the data which is requested by another node in the network or by changing the route of the packets. When the voting phenomenon occurs in the network then Sybil attacker can change the result by using its multiple identities behavior and make the result according to its requirement. So it is necessary to remove the Sybil attack from the network.

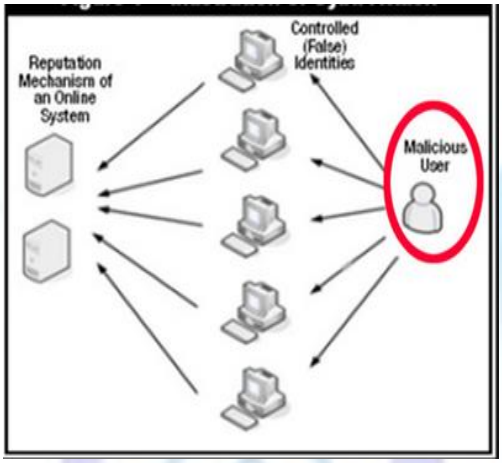

Fig1Representation of Sybil attack

In this paper, some prevention techniques are discussed to remove the Sybil attack from the network.

I. PREVENTION TECHNIQUES OF SYBIL ATTACK

A. Lightweight Sybil Attack Detection [2]

a. *Behavior of Sybil nodes:* Sybil nodes behave in two ways. In first type of behavior, it uses its one identity only at a time and eliminates all its earlier identities. It is called as join and leave and white washing attack. Its main motive Is to remove all previous bad actions performed by malicious nodes and it increases the irresponsibility in the network. In second type of behavior, attacker simultaneously uses all its identities called simultaneous Sybil attack and its main motive is to create interruption within the network and make efforts to get access of all information, data and resources in the network. In this step we make assumption that transmit power of nodes remain constant.

b. *Investigation based on Signal Strength*: On the basis of joining behavior of neighboring nodes we can distinguish between legitimate and Sybil nodes. At joining time RSS value of legitimate nodes is low whereas RSS value of Sybil nodes is high. In this information about neighbor nodes are collected by all the nodes i.e. RSS value in the form of <Address, Rss-List <time, rss> > as presented in Table1 [2]. On the basis of RSS value we can distinguish between Sybil and legitimate nodes.

Table 1: List contains RSS value of neighbor nodes [2]

Node ID	Rss-List
1	R1 T1 → R2 T2 → R3 T3 ------> Rn Tn
2	
3	
	. . .
N	

c. *Expose of Sybil nodes*: Here threshold value of speed is taken, which is equal to 10m/s [2]. The speed of legitimate node is not greater than this threshold speed. If the speed of node is greater than threshold speed then it is detected as Sybil node. Sybil node is detected on the basis of RSS value and RSS value depends upon the speed of node. If the RSS value is greater than threshold value than it is considered as Sybil node otherwise as legitimate node. In this two algorithms [2] are used, complexity of Algorithm 1 [2] is *O*(1) and of Algorithm 2 [2] is equal to *O*(n).

B. Secure Prophet Address Allocation [3]

Prophet address allocation [4]: To allocate unique IP address to the nodes, it uses a partition function f(n) which is used to generate sequence of integers. Here partition function is based on fundamental theory used in number theory. The partition function is also called the stateful function [3] which is associated with the beginning state or node called seed. These seeds are used to generate different sequence of integers. These sequences should consist of following characteristics:

a) There should be a long gap between the numbers which is repeated again in the sequence.

b) The likelihood occurrence of the same number again in a sequence should be very less.

As number or integer calculation includes the allocated address or the addresses which has to be allocated, by following above two characteristics it escapes the battle among the occurrence of same IP address again. The disadvantage of prophet address allocation is that seed value remains same throughout the network, so it is possible for the malicious node to come to know about the seed value by acting as a new node and causes various attacks in the network like IP spoofing, State pollution and Sybil attack.

Secure Prophet Address Allocation: It is an advanced version of prophet address allocation.

a) *Authentication of seed value:* The value which is generated by the initial node in the network is called seed value. During the allocation of address to the nodes, the seed value remains same throughout the process. When a new node enters in the network, first of all it must be authenticate that it receives the seed value from the legitimate node but as the seed value remains same throughout the network so it is difficult to authenticate that seed value doesn't come from malicious node. So to get the unique address in the network, it depends upon the uniqueness of the exponential array which is explained in next step.

b) *Improvement*: In the prophet address allocation updates are done within the states when the address is allocated, and in secure prophet address allocation when the address is allocated, updates are flooded in the entire network.

In this, acknowledgement consists of four variables that are seed value, index of increasing exponential, exponential array, priority variable and the source address of the responder.

Exponential array: In this new node inherits the parameter from its ancestors to calculate its own address. Exponential array variable tells the relationship between the new node and its ancestors.

Priority Variable: The greater number represents the newness of the state and greater the number, the more priority state will have. The new node will choose the high state priority number variable and then add some arbitrary value to its priority to calculate its own address. When the address is calculated then it floods the acknowledgement about the priority variable in the entire network. All nodes in the network update their priority values.

Relationship among the variables is following:

X= f(a, i[1..n])

Where

X= Source address of the responder

a= seed value

c= index of exponential

p= priority

i[1..n]= Initial exponential array

r= arbitrary value select by the new node

Address of new node (y) is calculated as follows:

y= f(a, e[1..n])

where

$$e[j]= \begin{cases} i[j], & j<c \\ p+r, & j=c \\ i[j]=0, & j>c \end{cases} \quad [3]$$

By using above formulas, distinct addresses are computed for all new nodes. In this each node has unique address and no node will use each other's address for an attack, so like this it will prevent Sybil attack.

C. MC-DCA [5]

Distributed Certificate Authorities [6][7]: In this certificates are distributed to all nodes which are used as the proof for their identities and help to prevent the Sybil Attack.

TABLE I. Summary of Sybil Attack Mechanisms

Mechanism Name	Cost	Architecture	Summary
Lightweight Sybil Attack Detection	Cheap	Distributive	The nodes entering in the network with speed greater than the threshold speed are detected as Sybil nodes.
Secure Prophet Address Allocation	Cheap	Distributed	The Sybil attack is prevented as Unique addresses are allocated to each node in the network.
MC-DCA	Costly	Centralized	To prevent Sybil attack, the certificates containing identities are distributed to each node.
Robust Sybil Attack Detection	Cheap	Distributive	The nodes having the same path or pattern are detected as Sybil nodes.

Multiple Key Cryptography: In this public key cryptography concept is used. In this multiple keys are used to encrypt and decrypt the data. It is enforced on DCA. So combination of DCA and multiple key cryptography is called as MC-DCA. It increases the security of data and prevents Sybil attack.

D. Robust Sybil Attack Detection [8]

According to the algorithm used in this, there are various clusters and main focus is on the path of nodes. The nodes having the path almost similar to the existing cluster, those nodes are put into the corresponding cluster and the node whose path is totally different and does not match with any existing cluster, and then separate cluster is developed for that node. In this, two nodes does not have exactly the same path, if two nodes are having the same path then those nodes are detected as Sybil nodes. The similarity of the node's path is checked by their overlapping components that how much they are overlapped. The similarity of the path is checked as follows:

$$Sim(L_1,L_2)=\left(\frac{\sum_{i=1}^{k} T_{cmni}}{\max(T_{obs1},T_{obs2})}\right) * \left(\prod_{i=1}^{k} \frac{T_{ovli}}{T_{cmni}}\right) \quad [8]$$

Here L_1, L_2 are nodes

T_{obs1}= It is a duration when each node is noticed.

T_{cmni}= It is a duration when both nodes are observed in the observation table.

T_{ovli}= It is a duration when both nodes are observed at the same time and they co-exist in same area.

K= It is the number of times when both nodes are observed commonly.

The first part of equation is used to calculate that till what time both nodes are observed commonly and second part of equation is used to determine the overlap region of the nodes.

III. CONCLUSION

In this paper some prevention measures are discussed to prevent the Sybil attack from the network. Sybil attack causes so much destruction in the network by changing its identities, so it is very necessary to remove this attack from the network and have secure communication in the network.

IV. REFERENCES

[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] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kasif Khifayat,``Lightweight Sybil Attack in MANETs,'' IEEE System Journal , Vol.7, No.2, pp.236-248, June 2013.

[3]Hongbo Zhuo,``Secure Prophet Address Allocation for Mobile Ad-hoc Networks'' IFIP International Conference on Network and Parallel Computing, pp.60-67, 2008.

[4]H.Zhuo,L.M.Ni,and M.W.Mutka``Prophet Address Allocation for large Scale MANETs'' In Proceedings of The 22nd Annual Joint Conference of IEEE Computer and Communication Societies(INFOCOM 2003),San Francisco,CA,April 2003.

[5]Hongbo Zhou,Matt W.Mutka,and Lionel M.Ni``Multiple-Key Cryptography-based Distributive Certificate Authority in Mobile Ad-hoc Networks "IEEE Globecom, pp.1681-1685, 2005 .

[6] Sarosh Hashmi, John Brooke,``Towards Sybil Resistant Authentication in Mobile Ad-hoc Networks Fourth International Conference on Emerging Security Information,System and Technologies, pp.17-24, 2010.

[7] Sarosh Hashmi, 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.

[8] Athichart Tangpong, George Kesidis, Hung-yuan Hsu,Ali Hurson,``Robust Sybil Detection for MANETs '' IEEE, 2009.

[9]IETF Mobile Ad-hoc Networks Group (MANET), IETF website www.ietf.org/dyn/wg/charter/manet-charter.html.

[10] Jin-Hee Cho,Ananthram Swami,and Ing-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.

Author' biograbhy

Roopali Garg

Roopali Garg is Coordinator of department of Information Technology Engineering at UIET, Panjab University, Chandigarh. She has an experience of 10 years in academics. She has done M. tech in Electronics and B. Tech in Electronice & Electrical Communication from Punjab Engineering College. She has been awarded Administrator's Gold medal by Chandigarh Administration in 2000 for her supreme performance in curricular, co- curricular and extra- curricular activities. There are more than twenty research papers to her credit which have been published in good indexed international journals and presented in reputed international conferences. Her focussed research area is Wireless communication and has guided more than a dozen M. thesis in this area.

Himika Sharma

Himika Sharma is research scholar of department of Information Technology at UIET,Panjab University,Chandigarh. She is pursuing her M.E. in Information and Technology from UIET,Panjab University,Chandigarh and has done B.tech in Computer Science from Punjab Tehnical University. Her main interests are ad hoc networks and wireless networks and currently working on improvement of security in mobile ad hoc networks.