# Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack

Himadri Nath Saha # [1] , Dr. Debika Bhattacharyya # [2] , Dr. P. K.Banerjee *[3]

Assistant Professor # [1], Professor # [2], 3 Professor *[3]
Department of Computer Science and Engineering, Institute of Engineering and Management, West Bengal, India # [1, ] # [2]
Department of Electronics and Communication Engineering, Jadavpur University, West Bengal, India *[3]
him_shree_2004@yahoo.com # [1], bdebika@yahoo.com# [2]

***Abstract:*** *Sybil attack is a serious threat for today's wireless adhoc networks. In this attack a single node impersonates several other nodes using various malicious means. In this paper we attempt to provide a hybrid solution using a combination of two already proposed methods. According to this newly proposed method the total network will be dynamically divided into several subgroups, as more and more nodes will enter the network. Each subgroup will be under the super vision of a single node, a central authority. Each subgroup will also contain RSSI detector nodes.*

***Keywords:*** *Sybil ttack,MANET, RSSI authentication.*

## 1. Introduction

A mobile adhoc network is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. This particular nature of the network makes it vulnerable to various, sybil attack being one of them. With no logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity, it is always possible for an unfamiliar entity to present more than one identity, except under conditions that are not practically realizable for large-scale distributed systems. Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems replicate computational or storage tasks among several remote sites to protect against integrity violations (eg. data loss). Others fragment tasks among several remote sites to protect against privacy violations (data leakage). In either case, exploiting the redundancy in the system requires the ability to determine whether two ostensibly different remote entities are actually different.Firstly all the messages in the network are of broadcast nature; secondly the network has no fixed infrastructure. If a good number of nodes are compromised then the network may totally collapse. Trusted Certification is one of the proposed solutions to sybil attack which requires a central trusted authority. Another proposed solution to this problem is an RSSI (Received Signal Strength Indication) based solution in which the physical location of the nodes are calculated. In this paper we attempt to combine the two proposed methods into a more efficient and practical solution to thwart the sybil attack.

## 2. Related Work

### *A. Trusted Certification*

One solution to the sybil attack is to assign unique node-Ids to each node in the network with the help of a central trusted authority. We use a set of trusted certification authorities (CAs) to assign node-Ids to principals and to sign node-Id certificates, which bind a random node-Id to the public key that speaks for its principal and an IP address. The CA's ensure that node-Ids are chosen randomly from the id space, and prevent nodes from forging node-Ids. Furthermore, these certificates give the overlay a public key infrastructure, suitable for establishing encrypted and authenticated channels between nodes. None of the known solutions to node-Id assignment are effective when the overlay network is very small.

For small overlay networks, we must require that all members of the network are trusted not to cheat. Only when a network reaches a critical mass, where it becomes sufficiently hard for an attacker to muster enough resources to control a significant fraction of the overlay, should mistrusted nodes be allowed to join.

## 3. B. RSSI Based solution

In this solution there is a detector node that calculates the RSSI ratio for each pair of nodes in the network. Suppose D1, D2, D3, D4 be the detector nodes and let a compromised node have 2 IDs S1 and S2. At time t1, a sybil node broadcasts a message with its forged ID as S1. Monitoring nodes record the RSSI and the forged ID. Each monitoring node sends a message to D1 containing the received RSSI from S1. Let Rki denote the RSSI value when a message from a sender k is received at i. Then, accumulating the messages from the monitors, D1 computes each ratio

*(Rs1d1/Rs1d2), (Rs1d1/Rs1d3)* and *(Rs1d1/Rs1d4)*

and stores them locally. At time t2, the sybil node broadcasts a message again with a different ID, S2. The monitoring nodes record the RSSI from S2 and report to D1. D1 computes each ratio as before:

*(Rs2d1/Rs2d2), (Rs2d1/Rs2d3)* and *(Rs2d1/Rs2d4)*

Now, D1 can detect the sybil node by comparing the ratio at time t1 and t2. If the difference between two ratios is very close to zero, D1 concludes that a sybil attack occurred in the region. Since RSSI ratios are same, the location is in fact the same for the alleged multiple IDs. Otherwise, D1 concludes that there is no sybil node. That is, if

*((Rs1d1 / Rs1d2) = ( Rs2d1 / Rs2d2))*
*((Rs1d1 / Rs1d3) = (Rs2d1 / Rs2d3))*
*and ((s1d1 / Rs1d4) = (Rs2d1 / Rs2d4))*

is true, then D1 detects a sybil attack.

## 4. The Proposed semi - centralized Solution

**Description of Notations:**

**Inputs provided**:

- V → Velocity of the central authority C
- R → Approximate radius of area occupied by a single node in the subgroup

## Output:

- N → approximate threshold value of the subgroup

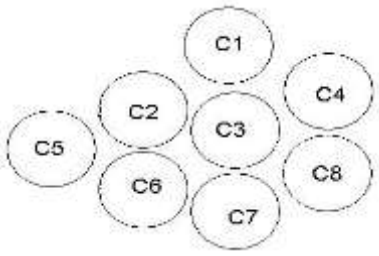


Fig.1 → Total network divided into logical subgroups
Ci = Central authority of each subgroup

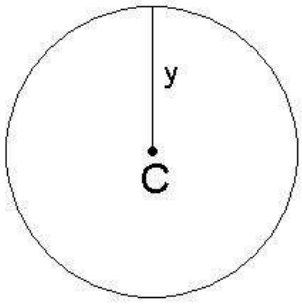


Fig.2 → Each subgroup
C = Central authority of the subgroup
y = distance of C from farthest node in subgroup

We have tried to combine the above two solutions in generating a new solution to detect Sybil nodes in a network. The main disadvantage of the central authority based solution is that it is

a centralized solution which is not entertained in ad hoc networks and will be a serious bottleneck when network size increases. The second solution which is a hardware based solution is approximate in nature and must be verified before any node can be removed from the network, thus requiring something like a central authority.

The biggest disadvantage of any central authority based scheme is that if the central authority is compromised, the whole network falls apart and all nodes become vulnerable to the malicious nodes.

As we know that the only way to somehow eliminate Sybil attack is to implement a central authority based scheme, we have tried to distribute the authority of this central node as far as possible. We assume that the total network will be dynamically divided into several subgroups as more and more nodes will enter the network. Each subgroup will be under the super vision of a single node, a central authority. Each subgroup will also contain RSSI detector nodes. The number of nodes for each subgroup is dynamically calculated taking in consideration the mobility of the central authority and the terrain where the subgroup is present. Whenever the number of nodes exceeds this threshold value, a new subgroup will be created and a new trusted node will be assigned as the central authority of that subgroup. The solution may be algorithmically stated as follows:

1. The network starts with n number of nodes. One trusted node assumes the responsibility of central authority C.

2. C calculates the threshold value, which determines the maximum number of nodes that can be present in that subgroup. C assigns a suitable number of nodes as RSSI detectors $R_i$. The number of RSSI detectors required for the subgroup is calculated from the threshold value of the subgroup by the central authority.

3. He manually assigns a unique identity to each node present in the network, but does not monitor the nodes once an identity is assigned to them.

4. The $R_i$'s take over at this point of time. They constantly monitor all nodes in the network, calculating and comparing the ratios of the RSSI values obtained for each node by at least 2 $R_i$'s.

5. C has the responsibility to constantly monitor the $R_i$'s manually such that they are not compromised. If the $R_i$'s declare Sybil attack has occurred at a particular location, C manually checks whether the node is indeed a malicious node or not. Threshold value n is calculated in such a way that maximum time taken by C to travel across the subgroup is optimal (around 1 min).

6. If C finds out that accused node is indeed malicious, the node is removed and the identities that were being used by the node are marked as available.

7. A point of time will come when each subgroup gets saturated. At this point the central authority will appoint a new node as the central authority of a new node. Then it will redirect all new requests to join its own subgroup to the newly created subgroup. Each central authority will be synchronized with the new subgroup it has created. In this way the initial central authority will redirect a new node to the next subgroup. If that too is saturated then it will be redirected to the next and so on.

8. When a new node will enter the network and request to be registered with the network, it might happen that two central authorities with unsaturated subgroups will receive the request simultaneously and respond. At this point of time the new node will have the liberty to choose any subgroup arbitrarily.

## Derivation of Threshold Value:

### Inputs provided:

- V →Velocity of the central authority C
- R → Approximate radius of area occupied by a single node in the subgroup

**Output:**

- N → Approximate threshold value of the subgroup

The calculations are as follows:

$$V_1 = V*k_2 \quad (1)$$
$$y = V_1*k_1 \quad (2)$$

Where $k_1$ = maximum time taken by C to travel across the node.

$k_2$ = **Terrain constant** < 1 and is dynamically determined by the surrounding conditions and terrain of the subgroup. This is done as the velocity will reduce in those extreme conditions.
Y is maximum possible radius of the subgroup.

$$N = y^2 / R^2 \quad (3)$$

**Explanation:**

Since velocity of C is V, and $k_1$ is the maximum time to travel across the subgroup, value of y is $V_1*k_1$. Thus the area is $\pi y^2$. Area occupied by each node is $\pi R^2$. So number of nodes is given is given by dividing them and result is given in (3).

## 5. Conclusion

Our solution combines two robust solutions and hence is robust. But there are a few points of concern. Firstly if the adhoc network finally has n number of subnets then initially there must be at least n trusted nodes. Otherwise there is a chance that one of the certifiers become compromised, disrupting the entire group. Secondly if one of the detectors of a group is compromised there might be some trouble. The detector may send false RSSI readings, thus creating chaos in a group. But here the advantage is that even if this happens, the problem would be bounded within the particular group only. Hence the situation would never get out of hand. So we hope this solution would make adhoc networks more secure and efficient at the same time.

## References

1. M.Mohsin and R.Prakash, *ip address assignment in mobile ad hoc networks*.
2. C.E.Parkins and P.Bhagwat, *highly dynamic DSDV routing for mobile computers.*
3. C.Karlof and D.Wagner, *secure routing in wireless sensor networks: attacks and counter measures.*
4. M.Demirbas and Y.Song, *an RSSI-based scheme for sybil attack detection in Wireless Sensor Networks.*
5. A.Ghaffari, *vulnerability and security of mobile ad hoc networks.*
6. J.R.Douceur, *the sybil attack.*
7. B.N.Levine, C.Shield and N.B.Margolin, *a survey of solutions to the sybil attack*
8. M.Castro, P.Druschel, A.Ganesh, A.Rowstron and D.S.Wallach, *secure routing for structured peer-to-peer overlay networks*
9. J.Newsome, E.Shi, D.Song and A.Perrig, *the sybil attack in sensor networks: analysis & defenses.*
10. H.Yu, P.B.Gibbons and M.Kaminsky, *brief announcement: toward an optimal social network defense against sybil attacks*
11. Issa Khalil, Saurabh Bagchi, Ness B. Shroff, *MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks*
12. W. Zhang, G.Cao, *Defending against cache consistency attacks in wireless adhoc networks*

## Author Biographies

**Prof Himadri Nath Saha :**Prof. Saha is graduated from Jadavpur University.He did his post graduate degree from Bengal Engineering and Science university.He is Assistant Professor of Institute of Engg and Management .His research interest is security in MANET.

**Prof.(Dr)Debika Bhattacharyya**:

Prof.Bhattacharyya did Phd. From Jadavpur University in the dept. of ETCE. She is HOD in the Dept of CSE.Her research Interest is security in MANET

**Prof.(Dr) P. K. Banerjee:** Prof. Banerjee is retired professor of Jadavpur University in the dept. of ETCE. His research interest is security in MANET.