DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS

S.Sharmila[1], G Umamaheswari[2]

[1]Research Scholar, Anna university, Tamil Nadu, India, **hod@dit.psgtech.ac.in**
[2]Aissitant Professor, Department of ECE, PSG College of Technology, Tamil Nadu, India, **gumabhaskar@yahoo.co.in**

Abstract

Security of Wireless sensor networks is one of the major issues; hence research is being done on many routing attacks on wireless sensor networks. This paper focuses on Sybil method and its detection. When a node illegitimately claims multiple identities or claims fake id, is called Sybil attack. An algorithm is proposed to detect the Sybil attack. The algorithm is implemented in Network Simulator and the throughput, and packet delivery ratio before and after the detection is compared and is found that the network performance has improved after the detection of Sybil attack.

Index Terms: *Wireless Sensor Networks, AODV, Sybil attack.*

-- *** --

1. INTRODUCTION

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. The development of wireless sensor networks was motivated by military applications such as battle field surveillance. Today such networks are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Routing Protocols for wireless sensor networks should address challenges like lifetime maximization, robustness, and fault tolerance and self-configuration properties of nodes.

.

1.1 Motivation

In recent years, wireless sensor network is widely applied in the fields of military, medical care and forest monitoring etc. It has become the hotspot. Because sensor nodes have limited storage and computational resources, it can easily be assaulted. Various types of attacks such as wormhole attack, sinkhole attack, selective forward attack, Sybil attack can be present in a network. A particularly harmful attack against sensor networks is the Sybil attack as this attack can make the network easily vulnerable to other attacks. Sybil attack is where a node illegitimately claims multiple identities. Now Sybil attack has caused too much threaten to wireless sensor network in routing, voting system, fair resource allocation, data aggregation and misbehaviour detection. Hence many methods are being proposed to detect and prevent Sybil attack in wireless sensor network.

2. SYBIL ATTACK

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities [6].

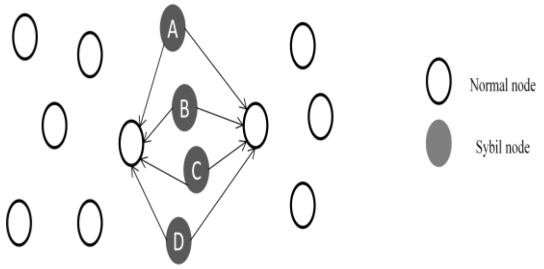


Fig-2.1 Sybil Attack

In fig 2.1 A, B, C, D is the Sybil nodes. When these nodes want to communicate to their neighbouring nodes they use any one of the identities. This confuses and collapses the network.

2.1 Types of Sybil Attack

In order to detect the Sybil attack it is necessary to understand the different forms in which the network is attacked [1].

(a) Direct and Indirect Communication:
In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, the communication is done through malicious node.

(b) Fabricated and stolen identities:
It creates a new identity for itself based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 32 bit integer, it randomly creates ID of 32 bit integer. These nodes have fabricated identities.

In stolen identities, attacker identifies legitimate identities and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

(c) Simultaneous and non-simultaneous attack:
In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous.

The number of identities the attacker uses is equal to the number of physical devices; each device presents different identities at different times.

2.2 Sybil attack on protocols

In a Sybil attack, a malicious node can generate and control a large number of identities on a single physical device. This gives the illusion to the network as if it were different legitimate nodes. It can affect the following important protocol[1]:

Distributed Storage The Sybil attack affects the architecture where it replicates the data on several nodes. Data will be stored on Sybil identities.

Routing Routing mechanism in which the nodes are supposed to be disjoint is affected by Sybil identities because one node will be present in the various paths and different locations at the same time.

Data Aggregation In sensor networks, data is grouped into one node to form complete information. When a Sybil node contributes many times posing as different users, the aggregated data changes completely thus giving false information.

Voting In WSN, most of the decisions are made by voting. Since the Sybil node has many identities, a single node has a chance of voting many times, thus destructing the process.

Misbehaviour detection: A Sybil node increases the reputation, credit, trust value by using its virtual identities. Thus the accuracy to detect a malicious node is reduced.

Fair resource allocation: Since the Sybil node has multiple identities it affects the allocation of resources. For example, when many nodes share a single radio channel, each node will be assigned a fraction of time per interval during which they can transmit. Since the Sybil node has many identities, it can obtain an unfair share of the resources thus reducing the actual share of resources to the legitimate node.

2.3 Existing Detection Methods of Sybil attack:

(a) Radio resource testing:
Consider that a node wants to verify that none of its neighbours are Sybil identities. It can assign each of its neighbours a different channel to broadcast some message on. It can then choose a channel randomly on which to listen. If the neighbour that was assigned that channel is legitimate, it should hear the message. Let‘s’ be the total number of the nodes ‘n’ be the number of Sybil nodes. The probability of detecting the Sybil node is s/n.

A more difficult case is when there are not enough channels to assign each neighbour a different channel. In this case, a node can only test some subset of its neighbours at one time. If there are ‘c’ channels, then the node can test ‘c’ neighbours at once. Note that a malicious node not in the subset being tested can cover for a Sybil node that is being tested by transmitting on the channel that the Sybil node is supposed to be transmitting on.

(b) Registration:
One obvious way to prevent the Sybil attack is to perform identity registration. A difference between peer-to-peer networks and wireless sensor networks is that in wireless sensor networks, there may be a trusted central authority managing the network, and thus knowing deployed nodes. The central authority may also be able to disseminate that information securely to the network. . To detect Sybil attacks, an entity could poll the network and compare the results to the known deployment. To prevent the Sybil attack, any node could check the list of “known-good’’ identities to validate another node as legitimate. Registration is likely to be a good initial defence in many scenarios, with the following

drawbacks. The list of known identities must be protected from being maliciously modified. If the attacker is able to add identities to this list, he will be able to add Sybil nodes to the network.

(c) Position Verification:

Another promising approach to defending against the Sybil attack is position verification. Here we assume that the sensor network is immobile once deployed. In this approach, the network verifies the physical position of each node. Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that generates them. By placing a limit on the density of the network, in-region verification can be used to tightly bind the number of Sybil identities that a malicious node can create.

(d) Based on RSSI:

By having the position of the nodes based on signal strength, we can find whether there is Sybil attack or not in wireless sensor networks [2]. Initially all the nodes have the same power, computing capability and the positions of nodes are fixed. The network is safe when the nodes are initialised using the signal strength. The disadvantage is the nodes are time varying.

2.3.1 Disadvantages

Each of the defences against the Sybil attack that we have examined has different tradeoffs. Most defences are not capable of defending against every type of Sybil attack. Additionally, each defence has different costs and relies on different assumptions. The radio resource verification defence may be breakable with custom radio hardware, and validation may be expensive in terms of energy. Position verification can only put a bound on the number of Sybil nodes an attacker can generate unless it is able to very precisely verify node positions. Node registration requires human work in order to securely add nodes to the network, and requires a way to securely maintain and query the current known topology information.

3. PROPOSED DETECTION LGORITHM

It includes three phases in which the detection accuracy is increased when compared to the previous phase.

Phase 1

.

- Create a group of mobile nodes.
- One of the nodes is taken as base station.
- The base station sends HELLO packets to all the other nodes for topology verification.
- The nodes with minimum packet drop are chosen as the trust nodes.
- The trust nodes now become the head nodes with a group of its own member nodes.
- The member nodes send their ID and power value to the head nodes.
- The head node checks for nodes with power value below the threshold value.
- If the power value is lesser than the threshold value, those nodes are detected as Sybil nodes.
- These abnormal nodes are selected as receivers for next detection phase

Phase II

- Two nodes closer to Sybil nodes are selected as senders s1, s2.
- Two Sybil nodes are selected as receivers r1, r2.
- Packets are sent to s1 and s2 to both receivers.
- Since both identities are present at the same node, there is collision of packets leading to packet drops.
- The distance between the receivers is found. If the distance is zero, the node suffers from Sybil attack
- if the nodes are very close, then the nodes will be detected as Sybil nodes even if they are not

Phase III

- The routing procedure in the cluster is checked to verify if there was a hop between the Sybil identities.
- If there exists a hop between the Sybil identities, then the nodes are not Sybil nodes.
- If no hops, then the nodes are confirmed to be under attack and they will be removed from the network. Two nodes closer to Sybil nodes are selected as sender’s s1, s2.
- Two Sybil nodes hop between the Sybil identities, and then the nodes are not Sybil nodes.
- If no hops, then the nodes are confirmed to be under attack and they will be removed from the network.

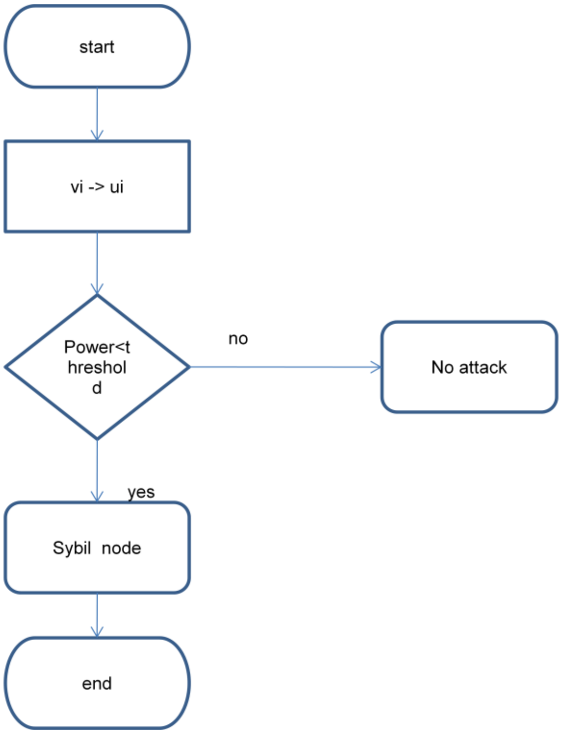


Fig- 3.1: shows the flowchart for phase -1

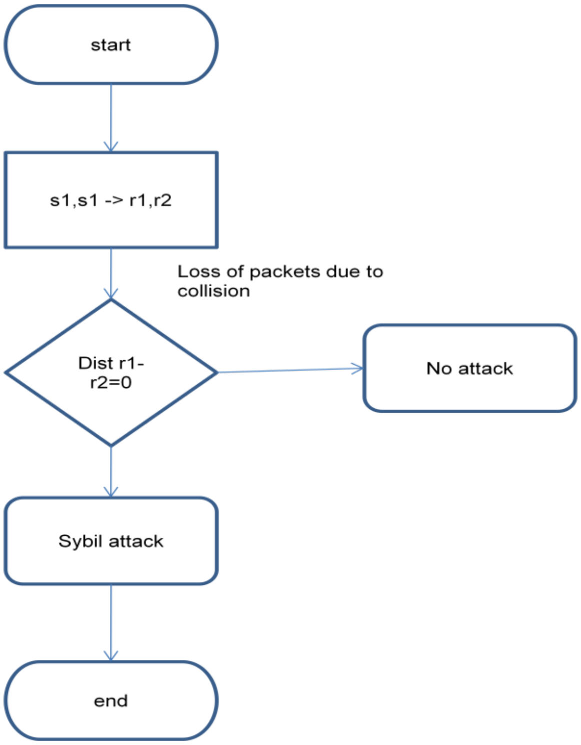


Fig-3.2: Flowchart for the Phase -2

Fig 3.1 and Fig 3.2 shows the flowchart for phase when a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally

4. PERFORMANCE EVALUATION

The proposed algorithm is implemented in NS2 and the performance is evaluated in terms of network throughput, packet delivery ratio, and packet drop.

A. Simulation Parameters

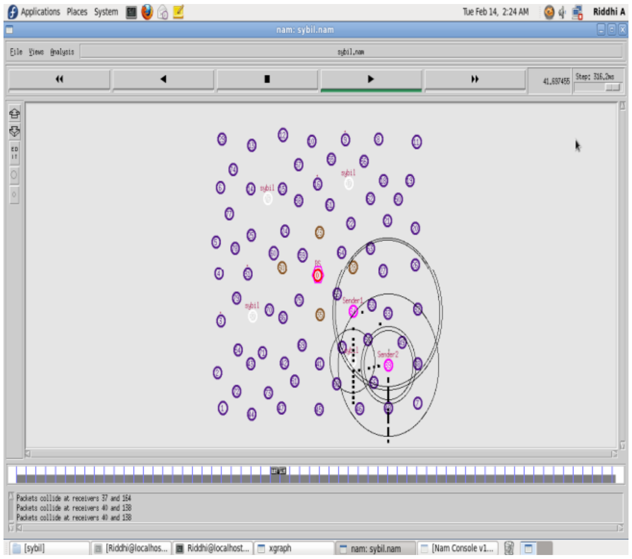
The parameters used in our simulation are shown in Table-4.1. A few nodes are selected and given multiple identities which act as Sybil nodes.

Table-4.1: Simulation Parameters

Area	10000mX10000m
Nodes	80
Packet size	512 bytes
Transmission protocol	UDP
Application Traffic	CBR
Simulation time	100 sec
Queue type	Drop tail
Propagation model	Two Ray Ground
Antenna model	Omni directional antenna
Routing protocol	AODV
Initial energy	100 Joules
Type of attack	Sybil attack

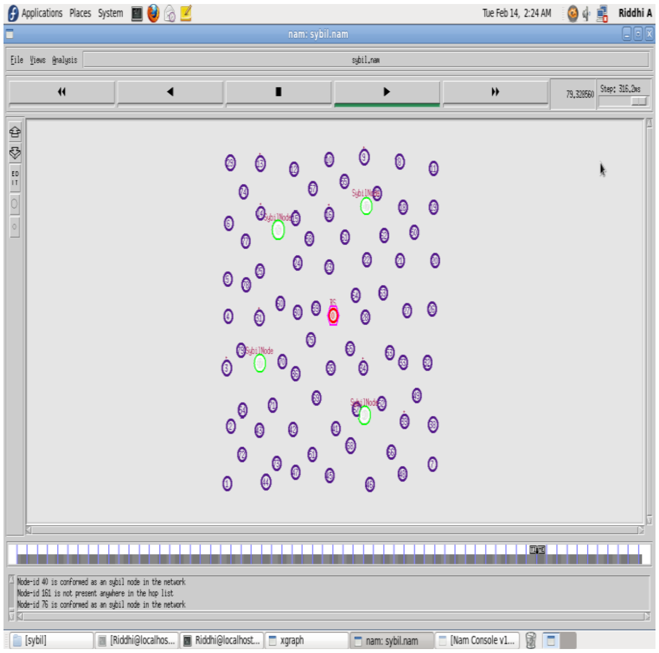
B. Simulation Results

In this section, the performance of the proposed detection algorithm is analysed in terms of network throughput and packet delivery ratio. Fig 4.1 and Fig 4.2 shows the packet drop and malicious node detection respectively.



```
Packets collide at receivers 37 and 164
Packets collide at receivers 40 and 138
Packets collide at receivers 40 and 138
```

Fig-4.1: Packet drop in the network



```
Node-id 40 is conformed as an sybil node in the network
Node-id 161 is not present anywhere in the hop list
Node-id 76 is conformed as an sybil node in the network
```

Fig-4.2: Sybil nodes are detected

The number of nodes created is eighty and node 0 is the Base station. After topology verification by the base station by sending ‘hello’ packets, the trust nodes are selected which are node 35, 30, 23, and 28 because they have minimum packet drop. The remaining nodes select the closest trust node as their Head node. Nodes 17, 37, 40, 76 are detected as Sybil nodes in the first phase. Two nodes closer to these nodes are taken as senders for second phase. Nodes 39, and 34 are selected as senders for node 37 and similarly. Finally third phase is implemented for the confirmation of Sybil nodes.

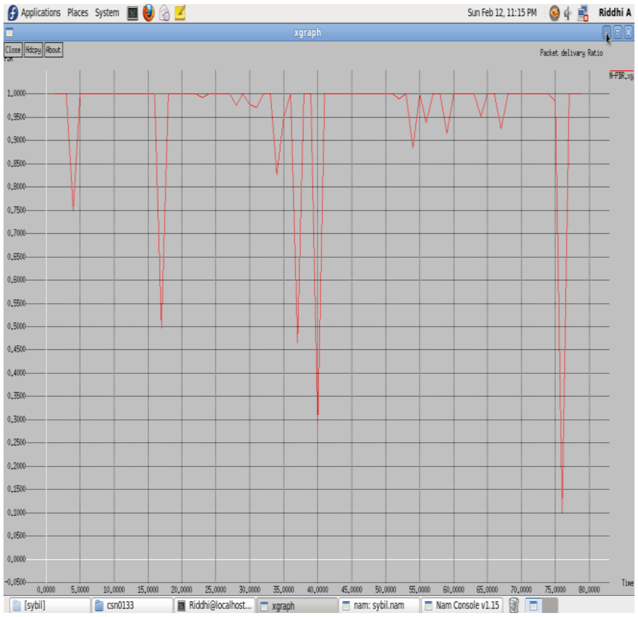


Fig-4.3: Packet Delivery Ratio before detecting Sybil nodes

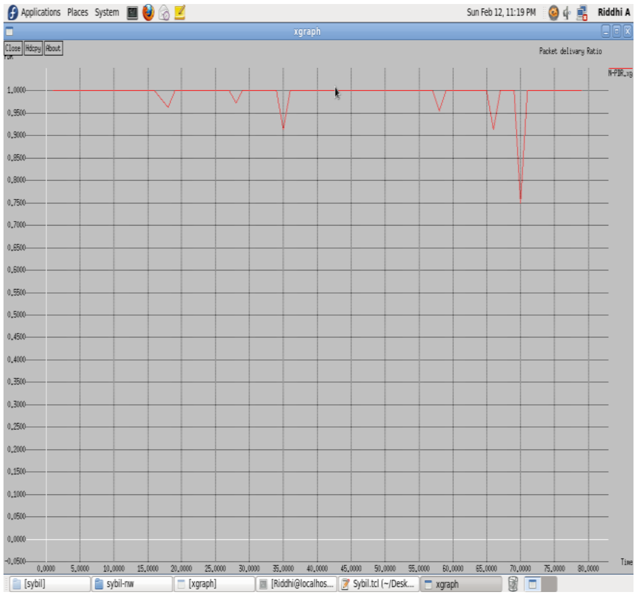


Fig-4.4: Packet Delivery Ratio after detecting Sybil nodes.

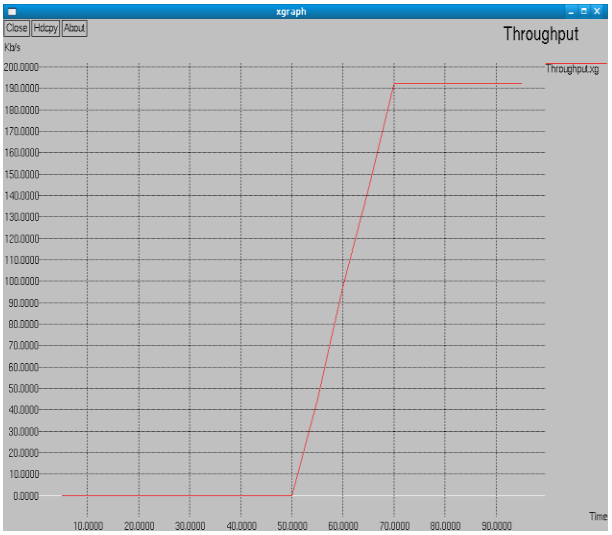


Fig- 4.5: Network Throughput before detection

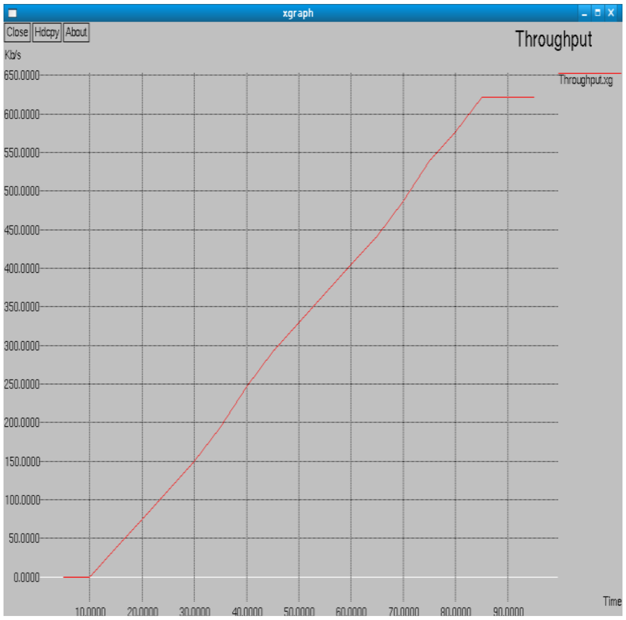


Fig- 4.6: Network Throughput after detection

The number of packets sent and throughput vary due to the presence of malicious nodes and is shown in Fig 4.3, 4.3,4.5,4.6 respectively. After detection, from the above graphs, it can be observed that the packet delivery ratio and throughput has improved in the networka node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally.

5. CONCLUSION

A number of existing methodologies for the detection of Sybil attack have been studied and an algorithm is proposed for detection of Sybil attack in wireless sensor network. The throughput and packet delivery ratio of the network, before and after detection is analysed for different traffic rates. It is found that throughput and packet delivery ratio after detection has improved.

REFERENCES

[1]. J. Newsome, E. Shi, and D. Song, “The Sybil Attack in Sensor Network: Analysis & Defences,” The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN’04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.

[2]. D. Murat, and S. Youngwhan, “An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks,” World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. International Symposium, 2006, pp.259-268.

[3]. J.Wang, G. Yang, Y. Sun, and S.Chen, “Sybil attack detection based on RSSI for wireless sensor network,” WiCom ’07: International Conference on Wireless Communications, Networking and Mobile Computing, September 2007, pp. 2684-2687, 21-25.

[4]. L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, “Detecting the Sybil Attack Cooperatively in Wireless sensor Networks,” in International Conference on Computational Intelligence and Security, CIS ’08. Vol.1 2008, pp.442-446.

[5]. Z. Qinghua, W. Pan, S. Douglas, and P Ning, “Defending against Sybil attacks in sensor networks,” Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshop (ICDCSW’05), 2005, pp.185-191.

[6]. J.R. Douceur. The Sybil attack. In First International Workshop on Peer-to Peer Systems (IPTPS’02), Mar. 2002.

[7]. Weichao Wang, Di Pu and Alex Wyglinski. Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding. IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), 2010.

[8]. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 2003, 1(2-3):293-315.

[9]. Chen, Geng Yang and Shengshou Chen. A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks. International Conference on Communications and Mobile Computing, 2010.

[10]. S.Abbas, M.Merabti, and D.Llewellyn-Jones. Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks. Second International Conference on Developments in eSystems Engineering, 2009.

[11]. Qiu Hui-Min. “Principle of Sybil attack and the defence,” Network and Computer Security, vol 10, pp.63-65, October 2005.

BIOGRAPHIES

S.Sharmila received the B.E and M.E degrees in Electronics and Communication Engineering and Applied Electronics from Bharathiyar University and Anna University, India in 1999 and 2004 respectively. Her research interest includes wireless sensor networks, computer networks and security.

G. Umamaheswari is Assistant professor in Electronics and Communication Department, PSG College of Technology, Coimbatore, India. She completed her B.E. degree in Electronics and Communication from Madras University in 1989 and M.E. in Electronics Engineering from Anna University, in 1992. She is now supervising 5 Ph.D. candidates