ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Detection of Sybil Attack in Wireless Sensor Networks

Manoj. R, Rajakumar. V. J, Caroline Mary. A

M. Sc Student, Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, India

Assistant Professor, Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, India

Assistant Professor, Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, India

ABSTRACT: A wireless sensor network (WSN) is a collection of sensor nodes, each of which is small, lightweight and less memory. These sensors are used to monitor physical or environmental conditions. In WSN these sensor nodes are subjected to SYBIL ATTACK. A Sybil attack consists of an adversary assuming multiple identities to defeat the trust of an existing reputation system which leads to a false routing, security issues. This paper attempts to provide an overcome measure against Sybil attack. The proposed system deals with use of UUID to find out the Sybil node in the network and even it provides security to transmit data between nodes using symmetric key algorithms. Hence the proposed system provides detection against Sybil node and security for transmission of data in the network.

KEYWORDS: SYBIL NODE detection; WSN; data transmission security;

I. Introduction

Wireless sensor network has become a popular technology due to its wide range of applications in military and civilian domains [1]. WSN is a collection of small, lightweight sensor nodes which are used to monitor physical or environmental conditions and various other applications. Each node can send messages through the network to the information sink – or ultimate controlling device. The nodes can also forward messages from other nodes, perform network organization tasks, and a variety of other functions [2]. Sensor nodes transmit data among other nodes in the network. Hence these sensor nodes are subjected to various attacks like sinkhole attack, wormhole attack, jamming and Sybil attack, etc,. This paper deals about a SYBIL ATTACK which is a one of the hardest attack to eradicate and it take place in the network layer of the WSN architecture. Sybil attack is an attack where a node pretends to be some other node with different identities.

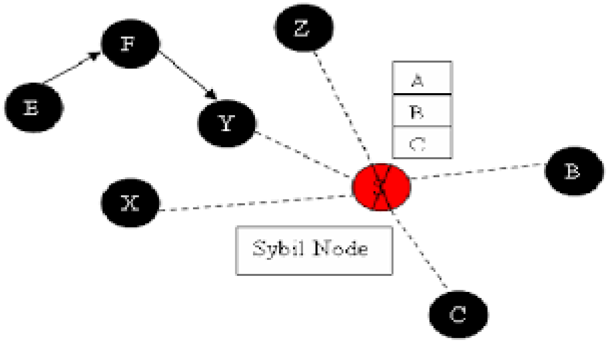


Fig. 1. Wireless sensor network with SYBIL NODE

Fig.1 represents a malicious node S along with its four Sybil nodes (A, B and C). 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 five different nodes. But in actual, there exists only one physical node with multiple different IDs. There different types of Sybil attack namely ROUTING – where the nodes are supposed to be disjoint is affected by Sybil identities because one node will be present in various paths and different location at the same time, FARE RESOURCE ALLOCATION – Sybil node has multiple identities it affects the allocation of resource and NETWORK

MISBEHAVIOUR - Sybil node increases the reputation, credit, trust value, so detecting a malicious node is reduced. To detect this Sybil attack unique Id where used. Symmetric key cryptography algorithm is used to provide security for data which is being transmitted among nodes in networks.

The following goals must be fulfilled by security algorithm used to detect the attack:

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

II. Related work

In [3] Sybil secure, a cluster head has parameters (identities and location) of each of its sub node and it queries to each sun node in network. Each node responses to query along with its identity and location based on it Sybil node can be detected but this technique is not suitable for large networks because of high traffic. RSSI based scheme presents a solution for Sybil attack based on received signal strength indicator (RSSI) readings of messages. Though it is said to be lightweight (i.e., only one message communication), it is time varying, unreliable and radio transmission is non-isotropic [4]. Accuracy reduces as transmission distance increases. Even there are some drawbacks of using MAC addresses for identification, where it is effective only in local network and packet forwarding is subjected to risk due to MAC spoofing attack.

In [5] author uses cryptography technique to detect the Sybil node. Each node is assigned with a key, a node which wants to send data uses the secret key to encrypt the data and passes the encrypted message along with the secret key to the destination through intermediate nodes. An intermediate node which attempts to temper the data using a duplicate key, then it is treated as a Sybil node or else it is a normal node. Whereas this technique faces an altering of bits in a encrypted message or key and even false routing. In [6] [7] various tasks are distributed to all identities of the network in order to test the resources of each node and to determine whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. The drawback of this approach is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks. In [8] NDD algorithm (Near-Detection) is used for detecting Sybil attacks. This algorithm is used 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 in to correct destination.

III. Proposed algorithm

A. *Description of the Proposed Algorithm:*

Each node in the network is assigned with the universally unique identifier (UUID) and a secret key during the registration process of the network. Admin stores each nodes UUID and secret key. Universally unique identifier UUIDs version 4 is used because of its randomness. The total size of ID is 128 bits, out of it 122 were random bits and remaining 4 for version and 2 for reserved bits.

Step1: Every node request for its neighbouring nodes UUID.

Step 2: Then each node checks with its INFO_TABLE which contains neighbouring nodes UUID . If neighbouring nodes UUID mismatches, then it informs to the admin.

Step 3: If every UUID where unique, then a source node request for a destination node’s SECRET KEY for encryption from the admin.

Step 4: After getting destination node’s SECRET KEY the source node will encryption the data and transmit to the destination. Finally destination node decrypts the data with its SECRET KEY.

Symmetric key cryptographic algorithm is used to encrypt and decrypt data. Whereas symmetric key algorithm uses a single key (known as SECRET KEY), used for both encryption and decryption. NEW symmetric key algorithm [9] is used to perform encryption and decryption in this process because of its simplicity and it is well suited for small amount of data. The steps of the NEW symmetric key algorithm is.,

Step1: Generate ASCII value of the data and corresponding binary value (8 digits) of it.

Step2: Reverse the 8 digits binary value and divide it with the (4 digits divisor) as the key.

Step3: Now store the remainder in the first 3 digits & quotient in next 5 digits, therefore it as an encrypted data.

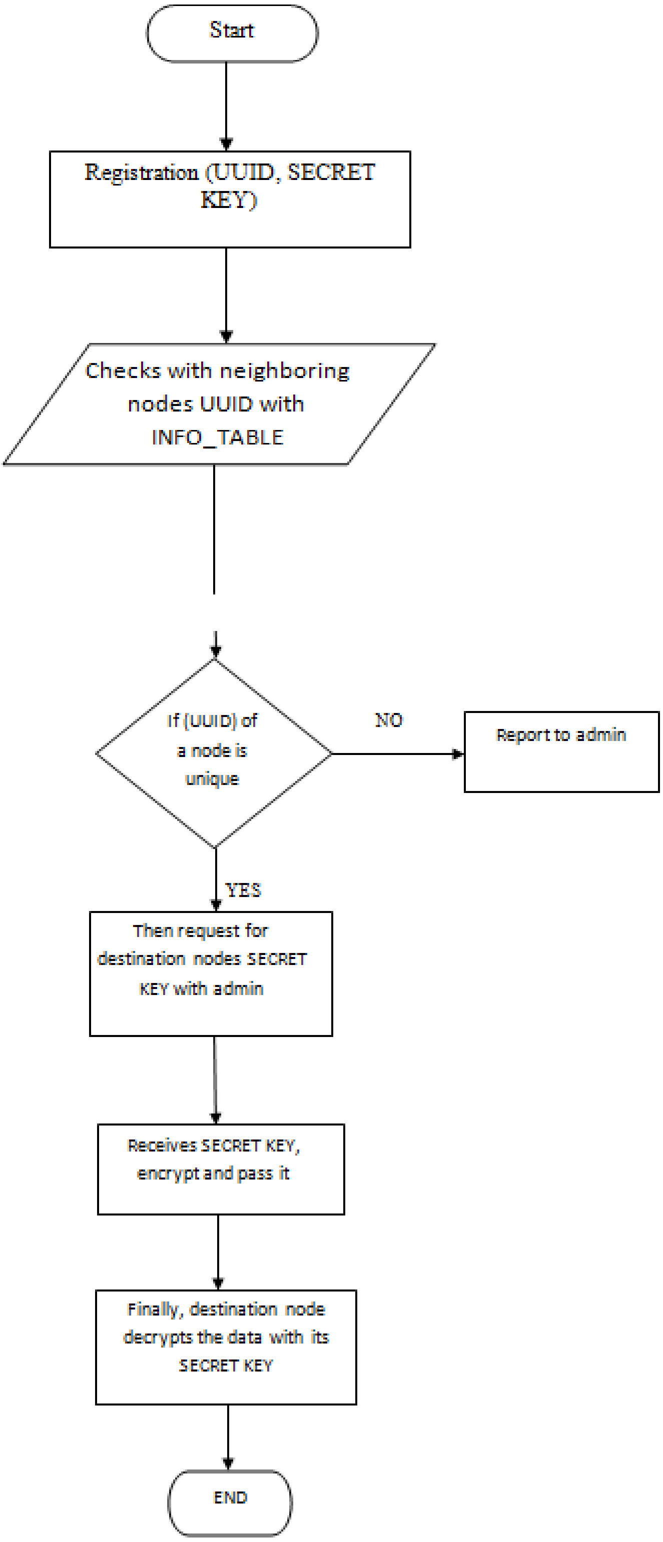
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

IV. Flowchart of a Proposed System


Start
Registration (UUID, SECRET KEY)
Checks with neighboring nodes UUID with INFO_TABLE
If (UUID) of a node is unique
NO
Report to admin
YES
Then request for destination nodes SECRET KEY with admin
Receives SECRET KEY, encrypt and pass it
Finally, destination node decrypts the data with its SECRET KEY
END

DOI: 10.15680/IJIRCCE.2016. 0408108

V. Conclusion and Future Work

Security is one of the foremost issues in WSN. In this paper a solution is proposed to detect the presence of Sybil node in the network and to transfer the data in the network in a secure manner. Where unique UUID of the node is used to identify the Sybil node and symmetric cryptography technique is used to encrypt and decrypt the data which ensures the message integrity. In future any other metrics can be used to identify the Sybil node in the network with improved performance.

REFERENCES

1. Vikash Kumar, Anshu Jain, P N Barwal ”Wireless Sensor Networks: Issues, challenges and solutions” International Journal of Information & computation Technology, volume 4, Number 8(2014), pp. 859-868.
2. R. Amuthavalli, DR. R. S. Bhuvaneswaran “Detection and Prevention of Sybil Attack in Wireless Sensor Network Employing Random Password Comparison Method” Journal of Theoretical and Applied Information Technology, Volume 67, No. 01(2014).
3. A. Babu karuppiah, A. Raja Prakash ”Sybil Secure: An Energy Efficient Sybil Attack Detection Technique in Wireless Sensor Network ” International Journal of Information Sciences and Techniques, Volume 4,No. 03(2014).
4. Anamika Pareek, Mayank Sharma “Detection and Prevention of Sybil Attack in MANET using MAC Address” International Journal of Computer Applications, volume 122, No. 21(2015).
5. Pankaj Rathee , Sona Malhotra “Prevention of Sybil Attack Using Cryptography in Wireless Sensor Networks” International Journal for Innovative Research in Science and Technology, Volume 2(2015).
6. Sangeeta Bhatti, Meenakshi Shrama “A Novel Algorithmic Approach for Detection of Sybil Attack in MANET” International Journal of Advanced Research in Computer Science and software Engineering, Volume 5(2015).
7. Sharmila.S, Umamaheswari.G “Detection of Sybil Attack in Mobile Wireless Sensor Networks” International Journal of Engineering Science and Advanced Technology, Volume 2.
8. Kavitha. P, Keerithana. C “Mobile-id based Sybil Attack Detection on the Mobile ADHOC Network”, International Journal of Communication and Computer Technologies, Volume 2(2014).
9. Ayushi “A Symmetric Key Cryptographic Algorithm” International Journal of Computer Applications, Volume 1,No. 15(2010).

BIOGRAPHY

R. Manoj pursuing his M. Sc Computer Technology in Sri Krishna Arts and Science College. His area of interest includes networks and java programming.

V. J. Rajakumar currently working as an Assistant Professor in Department of Computer Technology, Sri Krishna Arts and Science College. Coimbatore. His area of interest includes networks and data communication.

A. Caroline Mary currently working as an Assistant Professor in Department of Computer Technology, Sri Krishna Arts and Science College, Coimbatore. Her area of interest includes operating systems and network security.