Detection of Sybil Attack in Wireless Sensor Networks

Sonu.J.L, Dr. Kavitha Jaba Malar

M.phil Scholar Nanjil Catholic College of Arts and Science, Kaliyakkavilai, India
Assistant Professor Nanjil Catholic College of Arts and Science, Kaliyakkavilai, India

---***---

Abstract - ***A wireless sensor network (WSN) is a compilation of sensor nodes, each of which is small, trivial and a smaller amount memory. These sensors are used to check physical or ecological situation. In WSN these sensor nodes are subjected to Sybil attack. A Sybil attack consists of an adversary assume multiple identity to beat the trust of an existing standing system which lead to a false direction-finding, security issue. This work attempt to provide a conquer measure next to Sybil attack. The proposed work find out the Sybil node in the network and even it provide security to communicate data between nodes using symmetric key algorithms.***

Key Words: *Sybil Attack, ecological, Identities, Security.*

1. INTRODUCTION

Wireless sensor network has rotated out to be a trendy technology owing to its wide variety of application in military and civilian domain. WSN is a compilation of small, trivial sensor nodes which are used to screen physical or ecological situation and various other applications. Each node can send mail through the network to the in order sink or ultimate scheming device. The nodes can also forward mail from other nodes, perform network association tasks, and a variety of additional functions. Sensor nodes broadcast data among added nodes in the network. Hence these sensor nodes are subjected to a variety of attacks like sinkhole attack, wormhole attack, blocking and Sybil attack, etc, this work deals regarding a Sybil attack which is a one of the hardest attack to eliminate and it take place in the network layer of the WSN structural design. Sybil attack is an attack where a node pretends to be some other node with different identity. But in real, there exist only one bodily node with various different ids. There dissimilar types of Sybil attack namely routing where the nodes are supposed to be displace is affected by Sybil identities because one node will be there in various paths and different location at the same time, fare resource share Sybil node has many identity it affects the allocation of set aside system

2. Related Work

The cluster head has parameter of each of its sub node and it queries to each sun node in network. Each node responses to query along with its individuality and location based on it Sybil node can be detected but this method is not suitable for large networks because of high travel. RSSI based system presents a solution for Sybil attack based on conventional signal strength indicator (RSSI) readings of messages. Though it is said to be trivial, it is time varying, variable and radio broadcast is non isotropic. Accuracy reduces as transmission distance increase. The author uses cryptography method to detect the Sybil node. Each node is assign with a key, a node which wants to send data uses the secret key to encrypt the data and pass the encrypted message along with the secret key to the purpose through middle nodes. A middle node which attempt to anger the data using a copy key, then it is treated as a Sybil node or else it is a normal node. Whereas this method faces an altering of bits in an encrypted message or key and even false direction-finding. In a variety of tasks are dispersed to all identities of the network in order to test the capital of each node and to determine whether each self-governing node has sufficient capital to achieve these tasks. These tests are approved out to check the computational aptitude, storage skill and network bandwidth of a node. A Sybil attack will not have a enough amount of capital to perform the extra tests imposed on each Sybil identity. The drawback of this move toward is that an attacker can get enough hardware capital, such as storage, memory, and network cards to complete these tasks. In NDD algorithm (Near Detection) is used for detect Sybil attacks. This algorithm is used to transfer the data from basis to reason without any damage or loss as well as each node to have the neighbor's node address.

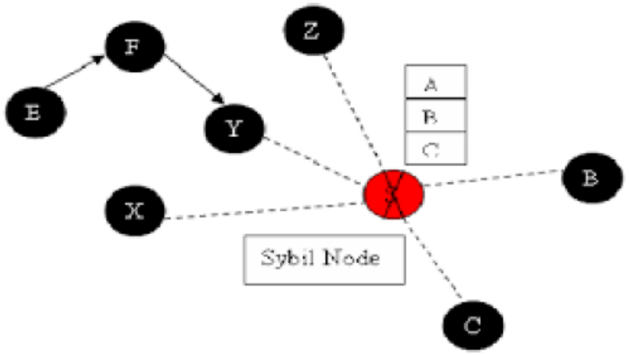

Fig. 1. Wireless sensor network with SYBIL NODE

This work deals regarding a Sybil attack which is a one of the hardest attack to eliminate and it take place in the network layer of the WSN structural design. Sybil attack is an attack where a node pretends to be some other node with different identity. But in real, there exist only one bodily node with various different ids. There dissimilar types of Sybil attack namely routing where the nodes are supposed to be displace is affected by Sybil identities because one node will be there in various paths and different location at the same time, fare resource allocation Sybil node has many identity it affects the allocation of reserve and network.

3. Proposed Methodology

Each node in the network is assigned with the generally unique identifier (UUID) and a secret key during the register procedure of the network. Admin stores each nodes UUID and secret key. Generally unique identifier UUIDs version 4 is used because of its chance. The total size of ID is 128 bits; out of it 122 were random bits and remaining 4 for version and 2 for kept bits. Every node request for its neighboring nodes UUID.Then each node checks with its INFO TABLE which contains neighboring nodes UUID. If neighboring nodes UUID mismatches, then it informs to the admin.If every UUID where unique, then a source node request for a purpose node's secret key for encryption from the admin.After getting purpose node's secret key the source node will encryption the data and transmit to the purpose finally destination node decrypts the data with its secret key. Symmetric key cryptographic algorithm is used to encrypt and decrypt data. While symmetric key algorithm uses a single key used for both encryption and decryption. New symmetric key algorithm is used to perform encryption and decryption in this procedure because of its ease and it is well suited for small amount of data. The symmetric key algorithm keys may be the same or there can be an easy transformation to go between the two keys. The keys, in practice, represent a shared secret between two or extra parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption .Make ASCII value of the data and corresponding binary value digits Reverse the 8 digits dual value and separate it with the (4 digits divisor) as the key. Now store the rest in the first 3 digits & quotient in next 5 digits, so it as an encrypted data.

4. CONCLUSION AND FUTURE WORK

Safety is one of the leading issues in WSN. In this paper an answer is proposed to notice the attendance of Sybil node in the network and to transfer the information in the network in a safe way. Any where unique UUID of the node is used to recognize the Sybil node and symmetric cryptography method is second hand to encrypt and decrypt the information which ensures the communication integrity. In prospect any other metrics can be used to recognize the Sybil node in the network with better presentation.

REFERENCES

1] Pankaj Rathee, Sona Malhotra "Prevention of Sybil Attack Using Cryptography inside Wireless Sensor Networks" International Journal Research in Science and Technology, Volume 2 (2015).

2] 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).

3] Sharmila.S, Umamaheswari.G "Detection of Sybil Attack in Mobile Wireless Sensor Networks" International Journal of Engineering Science and Advanced Technology, Volume 2.

4] Kavitha P, Keerithana C "Mobile-id based Sybil Attack Detection on the Mobile ADHOC Network", International Journal of Communication with Computer Technologies, Volume 2(2014).