Prevention of Sybil Attack using Cryptography in Wireless Sensor Networks

Pankaj Rathee
M. Tech Student
Department of Computer Science & Engineering
U.I.E.T, Kurukshetra University Kurukshetra, Haryana, India

Sona Malhotra
Faculty
Department of Computer Science & Engineering
U.I.E.T, Kurukshetra University Kurukshetra, Haryana, India

Abstract

Wireless sensor networks constitute of sensor nodes which are running on battery, small in size, limited memory, computation power and communication capability. Operational environment of sensor nodes is generally unfavorable and unattended which may result in failure of sensor nodes and they are prone to various malicious attacks. One of these attacks is Sybil attack. In this paper Sybil attack is prevented using cryptography. This paper shows the effect of Sybil attack in wireless sensor network and also shows the effect of proposed algorithm on network performance in presence of Sybil nodes.
Keywords: Sybil attack, Wireless Sensor network, Security, Key management

I. INTRODUCTION

Wireless sensor networks (WSNs) are a capable technology that can produce economically practical solutions to applications of different interests. WSNs have gain significant attention from both industrial engineers and researchers with numerous potential application domains such as health care and surveillance, smart buildings and Security and so on. However, most WSNs are deployed in open environment, which are mostly challenging which helps the security challenges to increase drastically. Broadcast nature of wireless communication made Security challenges in WSNs sever. In this paper, we studied the effect of Sybil attack on networks performance in absence of proposed of algorithm and presence of proposed algorithm. In Sybil attack a malicious node pretends to be multiple numbers of nodes being only a single node, for example by forging other nodes identities or by generating false identities. Newsome *et al.* [1] presented classification of different forms of Sybil attack, fabricated vs. stolen identities, Direct vs. Indirect communication, simultaneous vs. non-simultaneous participation. Figure 1 characterizes Sybil attack. In Sybil attack a Sybil node took or fabricates several identities and participates in network operations using these identities. It acts as if there are several members in the network being a sole physical device. It participates in all network operations on behalf of these Sybil identities. A Sybil node takes all data transmitted in network and transmits bogus data in network with these identities.

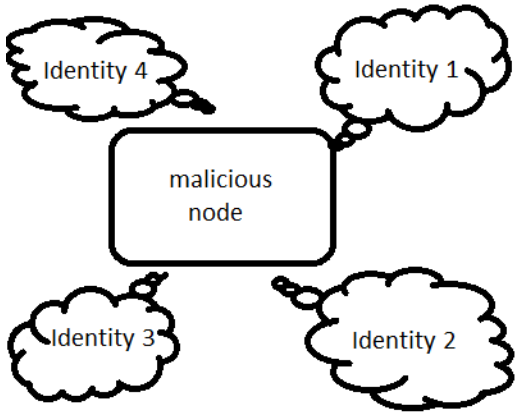

Fig. 1: Malicious node announcing its multiple identities

As a result of this network performance is degraded remarkably. The proposed system will be using cryptography to prevent Sybil attack. Due to power and computation restrictions of WSNs symmetric key cryptography is feasible in WSNs. Cryptography is a traditional way of authentication and confidentiality. Cryptography is a method of storing and transmitting data in encoded form so that only those for whom it is intended for can understand it. The proposed algorithm uses cryptography to prevent Sybil attack and improve network performance in presence of Sybil nodes.

II. RELATED WORK

A taxonomy of Sybil attack was presented in [1] by Newsome *et al.* They classified Sybil attack in different categories of fabricated or stolen identities, direct or indirect communication and simultaneous or non-simultaneous communication. [2] Proposed a key management protocol LEAP to defend against Sybil attack. LEAP uses four pair of keys. For local authentication LEAP used one way key chains. [3], [5] and [13] used location based methodologies to detect and defined Sybil attack. [3] Uses location based keys to design a compromise tolerant security system. Authors demonstrated the use of location-based keys in tackling a few blatant attacks against wireless sensor network routing protocols. In [5] authors developed an LBK-based neighborhood authentication scheme to localize the impact of compromised nodes to their vicinity. During the post-deployment phase, each node is required to discover and perform mutual authentication with neighboring nodes, which is a normal process in many existing security solutions for sensor networks. In [13] the proposed method detected Sybil attacks through anchor nodes location. The main idea behind this method was that two nodes cannot be present at same location at same time.
[6], [8], [10] and [11] uses received signal strength indication (RSSI) based methodologies. They all used the nodes signal strength to judge whether a node is Sybil in nature or not. [9] Proposed an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. [14] used both location and RSSI schemes to detect Sybil attack. During the evidence collection, observations related to location information, distance and RSS values are recorded. Whereas, in evidence validation, the computed evidences are submitted as inputs to sequential hypothesis testing to decide between two alternatives, neighbor node is a benign node and neighboring node is a Sybil node. [7] Proposed to utilize K-means cluster analysis for detecting Sybil attacks based on the spatial correlation between the signal strength and physical location. [15] Proposed a novel One Way Code attestation Protocol (OWCAP) for wireless sensors networks. [12] Proposed a secure neighbor authentication protocol based on a variant of HB, an authentication protocol for RFID devices. HB shared-key, unidirectional authentication protocols whose efficiency makes them potentially suitable for resource constrained devices such as RFID tags. [4] Offered light-weight identity certificate method to defeat Sybil attacks. Authors used one way key chains and two level merkle hash trees to create certificates.

III. PROPOSED ALGORITHM

A key management protocol is developed that will prevent Sybil attack in wireless sensor networks. Each node will be assigned individual keys for communication. In any communication one node's key will be used as source node key and another node's key will be treated as intermediate node key. These keys will also act as node id's. A Symmetric encryption scheme will be employed for encryption. The simulation work is done in ONE simulator. This key management protocol will provide a secure environment for communication and will prevent Sybil attack. This scheme uses symmetric cryptography which is computationally cheaper as compared to asymmetric cryptography so this protocol will be energy efficient. Sybil nodes affect working of WSN in many terms like, dropping packets, entering bogus routing data in network, throughput of the network. This work will show the effects of Sybil attack in wireless sensor network in terms of average message delay, number of messages delivered, number of messages dropped, overhead ratio and throughput. Proposed System uses Cryptographic ideas to detect and prevent the Sybil attack. Following sections explain different phases and algorithms used in proposed system.

A. Pre-Node Deployment Phase:

Each node will be assigned a node id prior to node deployment. The sensor nodes can be deployed via aerial scattering or by physical installation.

B. Sybil Node Detection Phase:

Following algorithm is used to detect the Sybil nodes present in wireless sensor network.

1) For (i=0;i<=n;i++)
   {
2) If ((msgid_source=msg_received by Node)&&(msg_received by Node = msg_forwarded by Node))
   {
   Then node status is set = "Normal node"
   }
   Else
   Node status = "Sybil Node"
}

Any node which will try to temper the data packets will be treated as Sybil node. This algorithm checks that if a node is forwarding the same data packets without tempering them then this node will be considered as normal node otherwise it will be considered Sybil node.

C. Proposed Algorithm for Sybil Node Prevention:

1) S_k = Sender Key
2) D_k = Duplicate Key
3) S= sender

4) IN= Intermediate node
5) M= message
6) N_i= Node
7) For(i=0;i<=n;i++)
8) {
9) Encrypt M with S_k
10) IN forward M with S_k
11) If IN haven't S_k
12) {
13) then it cannot forward the message
14) If IN apply an attempt to break S_k with its D_k
15) {
16) then N_i is Sybil.
17) }
18) else
19) N_i is Normal.
20) }
21) }

Here S_k is Sender Key, D_k is Duplicate Key, S is sender node, IN is used for Intermediate node, M is the message to be sent, N_i is the node we are currently checking for its Sybil behavior. Each message M will be encrypted with Sender Key S_k then this message will be forwarded by intermediate nodes with sender key S_k and if intermediate node doesn't have sender Key then it will not be able to message. If intermediate node attempts to break S_k with it duplicate key D_k then N_i will be treated as Sybil node otherwise it will be treated as normal node.

D. Methods To Encrypt/Decrypt Message:

Following methods will be used to encryption decryption and key generation.

1) Key generation:

```
private static Key generateKey() throws Exception {
      Key key = new SecretKeySpec(keyValue, ALGO);
         return key;
}
```

2) Encryption:

```
byte[] encVal = c.doFinal(Data.getBytes());
String encryptedValue = new BASE64Encoder().encode(encVal);
```

3) Decryption:

```
byte[] decordedValue = new BASE64Decoder().decodeBuffer(encryptedData);
byte[] decValue = c.doFinal(decordedValue);
```

IV. RESULT AND ANALYSIS

The performance of the proposed algorithm is estimated by comparing it with the performance of network in presence of Sybil attack without using this algorithm. The main motive of the work is to compare the two systems on the basis of effect on the network performance. So the results are evaluated on the basis of following parameters:

- Messages delivered
- Messages dropped
- Average message delay
- Overhead ratio
- Throughput

For the performance comparison, three scenarios are considered.

- Network having 20 nodes
- Network having 40 nodes
- Network having 60 nodes

In each case, a random number of nodes are considered as Sybil nodes each time so as to evaluate the network performance in the different cases in the network with presence of Sybil attack both in the without as well as with the proposed one.

The simulation results are shown in the form of various comparison graphs. The comparison is made between network performance in presence of Sybil attack with and without proposed algorithm.

A. Graph 1:

This graph shows the comparison between the number of messages delivered in network in presence of Sybil attack with and without proposed algorithm.

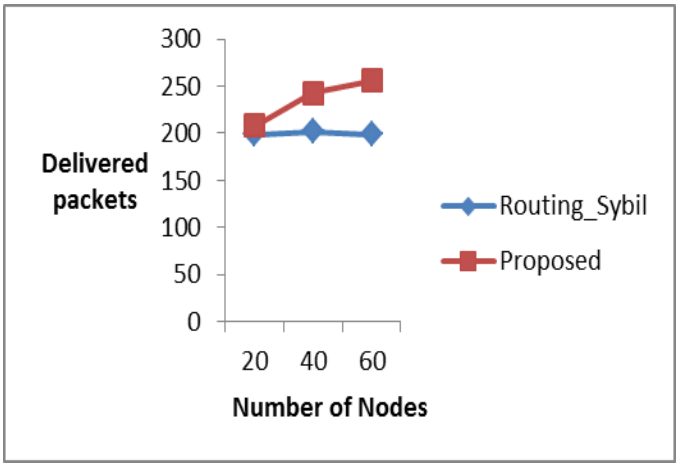

Fig. 1: Graph 7.1 Comparison of number of messages delivered in network

Routing_Sybil: Number of messages delivered in network without proposed algorithm
Proposed: Number of messages delivered in network with proposed algorithm

B. Graph 2:

This graph shows the comparison between the number of messages dropped in network in presence of Sybil attack with and without proposed algorithm.

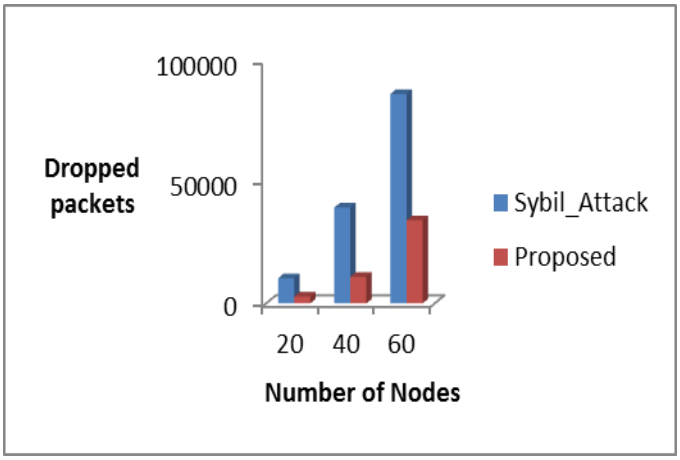

Fig. 2: Graph 7.2 Comparison of number of messages dropped in network

Routing_Sybil: Number of messages dropped in network without proposed algorithm
Proposed: Number of messages dropped in network with proposed algorithm

C. Graph 3:

This graph shows the comparison between average message delay in network in presence of Sybil attack with and without proposed algorithm.

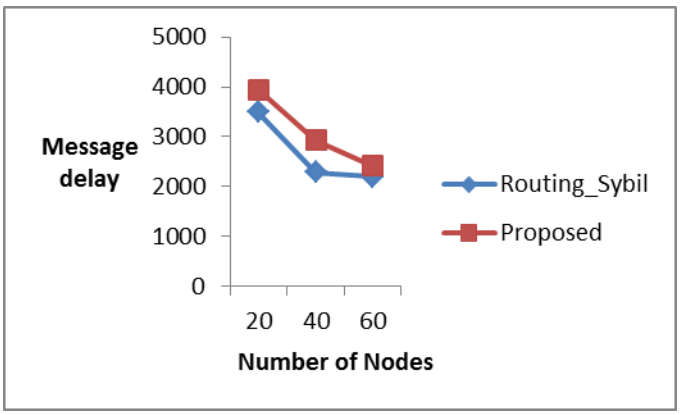

Fig. 3: Graph 7.3 Comparison of average message delay in network

Routing_Sybil: Comparison of average message delay in network without proposed algorithm
Proposed: Comparison of average message delay in network with proposed algorithm

D. Graph 4:

This graph shows the comparison between overhead ratio in network in presence of Sybil attack with and without proposed algorithm.

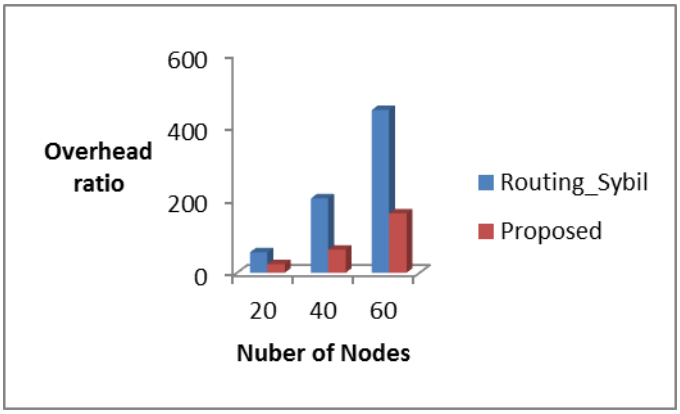

Fig. 4: Graph 7.4 Comparison of overhead ratio in network

Routing_Sybil: Comparison of overhead ratio in network without proposed algorithm
Proposed: Comparison of overhead ratio in network with proposed algorithm

E. Graph 5:

This graph shows the comparison between throughput of network in presence of Sybil attack with and without proposed algorithm.

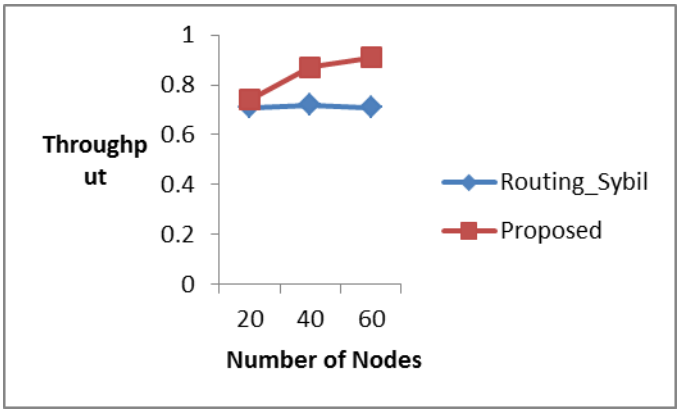

Fig. 5: Graph 7.5 Comparison of throughput of network

Routing_Sybil: Comparison of throughput of network without proposed algorithm
Proposed: Comparison of throughput of network with proposed algorithm

V. CONCLUSION

Wireless sensor networks are prone to various attacks in presence of scarce resources and insecure working environment. Security protocols made for wireless sensor networks must be forced to work within well-defined boundaries of wireless sensor networks. It must be energy efficient, computationally simple and shall consume less memory. The proposed key management protocol will provide a secure environment for communication and will prevent Sybil attack. The proposed algorithm helps in improving the network performance. The simulation results show that it improves number of messages delivered and dropped, throughput, and overhead ratio. Simulation results show that the technique is capable of improving the network performance but can still be improved further on average message delay.

REFERENCES

[1] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig "The Sybil Attack in Sensor Networks: Analysis & Defenses," ACM, Berkeley, California, USA. IPSN'O4, April 26-27, 2004.
[2] Sencun Zhu, Sanjeev Setia, Sushil Jajodia "LEAP: Efficient Security Mechanisms for LargeScale Distributed Sensor Networks," Tech report, ACM 2004.
[3] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang "Securing Sensor Networks with Location-Based Keys," in IEEE Conference on Wireless Communications and Networking, vol. 4, pp. 1909-1914, 2005.

[4] Qinghua Zhang, Pan Wang, Douglas S. Reeves and Peng Ning "Defending against Sybil attacks in sensor networks," in 25th IEEE International Conference on Distributed Computing Systems Workshops, pp. 185-191, june. 6-10, 2005.
[5] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," in IEEE Journal of Selected Areas in Communications, Vol. 24, Issue 2, pp. 247-260, Feb. 2006.
[6] Jiangtao Wang, Geng Yang, Yuan Sun, Shengshou Chen "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2684 – 2687, Sept. 21-25, 2007.
[7] Jie Yang, Yingying Chen, Wade Trappe "Detecting Sybil Attacks in Wireless and Sensor Networks Using Cluster Analysis," in 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Sept. 29 2008-Oct. 2, 2008.
[8] Shaohe Lv, Xiaodong Wang, Xin Zhao and Xingming Zhou "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks," in IEEE International Conference on Computational Intelligence and Security, Suzhou, Vol. 1. Dec. 13-17, 2008.
[9] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam "Channel-Based Detection of Sybil Attacks in Wireless Networks," in IEEE Transactions on Information Forensics and Security, Vol. 4, Issue 3, pp. 492 – 503, July. 07, 2009.
[10] Yingying Chen, Jie Yang, Wade Trappe and Richard P. Martin "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," IEEE Transactions on Vehicular Technology, Vol. 59 , Issue 5, pp. 2418 – 2434, March. 08, 2010.
[11] Shanshan Chen, Geng Yang, Shengshou Chen "A Security Routing Mechanism against SybilAttack for Wireless Sensor Networks," in IEEE International Conference on Communications and Mobile Computing, Shenzhen, April. 12-14, 2010.
[12] Jasmine Norman, Paulraj Joseph "Secure Neighbour Authentication in Wireless Sensor Networks," in 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Chennai, Feb. 28, 2011-March. 3, 2011.
[13] Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhaohui LIU and Changxing XU "A Novel Sybil Attack Detection Scheme for Wireless Sensor Network," in 5th IEEE International Conference on Broadband Network & Multimedia Technology, Guilin, Nov. 17-19, 2013.
[14] P. Raghu Vamsi and Krishna Kant "A Lightweight Sybil Attack Detection Framework for Wireless Sensor Networks," in IEEE 7th International Conference on Contemporary Computing, pp. 387 – 393, Aug. 7-9, 2014.
[15] Imran Makhdoom, Mehreen Afzal, Imran Rashid "A Novel Code Attestation Scheme Against Sybil Attack in Wireless Sensor Networks," in IEEE Nation conference on Software Engineering, pp. 1 – 6, Nov. 11-12, 2014.