ISSN: 0369-8963

Lightweight Trust Based Sybil Attack Detection Framework for Wireless Sensor Network with Cluster Topology

V. SUJATHA[*1], E.A. MARY ANITA [*2], D.VINODHA[*3]
*[*1] Research Scholar, AMET University, Chennai, India*
*[*2] Professor/ CSE, School of Engineering and Technology, Christ University, Bengaluru*
*[*3]Dr.D.Vinodha, Assistant Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Sriperumbudur*

Abstract

Due to the advancement in the communication and networking technologies, Wireless Sensor network plays eminent role in various domain. Because of the remote hostile characteristics of Wireless sensor networks, it is uncertain against various security attacks. One such harmful, yet easy to promote an attack is the Sybil attack which creates multiple identities to achieve access to the wireless sensor networks. A new identity and trust-based scheme to provide security against Sybil attacks is proposed in this paper. To improve the accuracy level of the attack, RSSI and location parameter are analyzed It detects as well as broadcast information about the attackers to all the nearby sensor nodes. It also provides other essential security features.

Introduction

Wireless Sensor Networks because of their intrinsic benefits like cheap in cost and easy to deploy in remote hostile region [7], play a vital role in a wide range of applications which include military surveillance [8], Building automation and monitoring [9], health care [10], and etc. However, the very miniature nature of sensor modes, makes the network to suffer from resource constrains like limited computing power, transmission power, memory and less energy [18]. The hostile nature of the region in which the Wireless sensor network displayed, makes the network prone to many attacks [16]. One of the most threatening attacks is Sybil attack. In the threat, the single harmful node affects the reputation of the network by operating many identities at one time and gains the influence of the network [17]. By forging the identities, the genuine nodes are misled and the performance of the network gets affected. Sybil attack was abstracted and projected by Douceur (2002) for peer-to-peer network. A Sybil node disrupts the service of the WSN by manipulating the decision of a voting mechanism in a group [15]. Hence, we propose to develop a framework to identify the presence of Sybil node with the help of trust-based certificate generated using Elliptic curve encryption along with the factors like location and received signal strength indicator (RSSI).

The paper is organized as follows: Section II presents a review of existing systems for detecting the Sybil attack in WSN. Our proposed work for detecting Sybil attack using certificate and RSSI is given in Section III. Results are discussed in section IV. Finally, in Section V, the conclusion is presented.

Related Work

The Various procedures of executing Sybil attack like direct and indirect transmission, stolen and fabricated identity and concurrent and non-concurrent attacks are presented by [1]. In direct transmission method, Sybil nodes participate in the transmission openly along with the original nodes whereas in indirect method intermediate nodes are employed by Sybil node by transmission. In the fabricated and stolen identity-based procedure, Sybil node imitate the truthful nodes by stealing their identity or fabricate new identity using the stolen one. In the concurrent and non-concurrent procedure, multiple

 https://doi.org/10.37896/pd91.5/91567

ISSN: 0369-8963

identities are created by Sybil nodes and are used for transmission all at one time or at different times.

In [2], the various approaches for initiating Sybil attack in WSN are discussed. The approaches are based on routing, data collection and disseminated storage. In the third approach base on disseminated storage, the attack is imposed by disintegrating or by duplicating the information. The duplicated identities are getting accumulated in base station. In routing-based approach, the data is diverted to multiple paths with Sybil node. In Data collection-based attack method, data is collected from the sensor node communicated to the base station

In [3], the author proposed a light weight scheme for detecting the intrusion based on the received signal strength indicator (RSSI).In this, RSSI is computed locally from the intruded node . The local computation does not require any communication [4]. Another scheme for detecting the Sybil attack based on identity and position is proposed in [4]. Trust is computed based on energy level. The performance is improved by employing data aggregation to minimize the communication cost in energy starving Wireless sensor network. But the trust only by using the energy parameter makes the system to suffer from the accuracy level of detecting the Sybil attack.

Arthanareeswaran et.al. in [5] proposed another method to detect Sybil attack using RSSI in Wireless sensor network deployed as clusters. Every node maintains a table structure and makes an entry about the message overheard including the RSSI. The presence of Sybil node in particular region is detected by analyzing the number of entries in the table. If it is visibly high compare to the other regions, then the presence of attack is concluded.

Another scheme proposed by Panagiotis et.al in [6] adopted rule-based anomaly scheme. it makes this framework suitable for large scale wireless sensor network. The scheme utilizes the detection algorithm based on ultra-wideband (UWB) range. It works in a decentralized manner without the need of data communication and coordination among the sensor nodes.

Nowadays, research is being carried out to mitigate Sybil attack to ensure secure communication over the WSN. Several approaches are based cryptographic functions are proposed to recognize Sybil attackers. The position-based approaches are utilized to recognize the Sybil nodes. RSSI is a significant factor utilized in most of the approaches to recognize Sybil nodes in the WSN. In this work, we propose to develop framework to detect the presence of Sybil node by merging the benefits cryptographic, position and RSSI based approaches.

Detection of Sybil Attack – Proposed Work

Network Model

Wireless Sensor Network with cluster tree topology is considered for deploying the nodes in our scheme. In this, the nodes are grouped into clusters based on the geographical location. All the communication inside the cluster is done through the nodes called cluster head (CH). The CH plays the role of cluster coordinator. The data sensed by the sensor nodes are communicated to CH or base station using a single hop or multiple hops. Fig 1 gives the network model based on cluster topology.

 https://doi.org/10.37896/pd91.5/91567

ISSN: 0369-8963

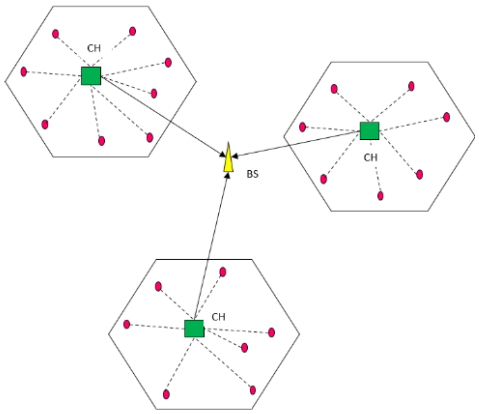

Fig 1 Network model

Node Setup

All the nodes are deployed with the Elliptic curve parameter G, n, q. Here, 'n' is a prime and 'G' refers to the generator of order 'n'. The public key 'k' used for generating the node authentication code is also deployed in the sensor node.

Certificate Generation Phase

The certificate for identifying the node communicating with, is generated by the CH for each node whenever request is received from communicating cluster member. The cluster member computes the R_i component $R_i = r_i * G$ using the random r_i. Node authentication code is computed using the public key of CH. It is transferred to CH along with node id, nonce, trust factor TF_i and its current location 'l'. This code is utilized by the CH for verifying the authenticity of node communicating with CH. Once the verification is successful, the CH generates the certificate using the equation given below

$$CT_i = (R_i + l + n_i + TF_i + r_{CHi} * G) \, mod \, n$$

Using one-way hash function 'c' is computed and it is used to compute 'd' as follows.

$$d = c * r_{CHi} + PR_{CH}$$

Then, the CH computes the node specific public key which is used for secure communication between CH and node 'i'. The certificate and'd' along with the component nonce is communicated to node 'i '. The node verifies the identity of CH by recomputing the node authentication code. After ensuring the identification, it computes its own private key by using the received certificate as follows.

$$PR_i = cCT_i + d \, mod \, n$$

Algorithm for generating certificate request, certificate and node specific private key is given below.

Algorithm 3.1

Generation of Certificate Request

1. A random element (r_i) is chosen from $\{1..n-1\}$ by the cluster member.
2. Compute $R_i = r_i * G$
3. Node Authentication code is generated (AU_i) using $R_i, node\ id, nonce$ using the public key k

https://doi.org/10.37896/pd91.5/91567

ISSN: 0369-8963

4. AU_i is communicated to CH along with $R_i, node\ id(n_i), nonce, l$. Where 'l' refers to the node location.

Generation of Certificate

1. CH verifies the identity of the node using AU_i . if the verification is successful, certificate for node n_i using the following steps
   a. Chose a random (r_{CHi}) from the node specific pseudo keys
   b. Certificate CT_i for the node n_i is computed as
      $((R_i + l + n_i + TF_i + r_{CHi}) * G)\ mod\ n$
   c. Compute $c = H(CT_i)$ where H is the one way hash function and compute $d = c * r_{CHi} + PR_{CH}$
   d. Compute Node Authentication code using the certificate $CT_i, nonce, d, and\ n_i$.
   e. $PB_i = cCT_i + k$
2. Certificate CT_i is communicated to the node along with $nonce$ and d

Generation of nodewise private key

1. The node verifies the authentication of CH by computing the node authentication code using the received certificate$CT_i, nonce, d, and\ n_i$.
2. If the verification succeeds, it computes $c = H(CT_i)$ and its own private key $PR_i = cCT_i + d\ mod\ n$

Notations	Descriptions
CT_i	Certificate of the node 'i'
AU_i	Authentication code
H	One way hash function
r_{CHi}	Random number generated at CH
r_i	Random number generated at node n_i
PR_{CH}	Private key of CH
K	Public key
l	Node location
PB_i	Public key of node 'i'
PR_i	Private key of node 'i'
TF_i	Trust factor of node 'i'
RC	Received Certificate
CT_{ri}^t	Certificate received from node ' i' at time 't'
CT_{ai}^t	Active certificate for node ' i ' at time t
Mu	Metric unit
Dt	Distance

Table 3.1 Notations

Detection of Sybil attack

Two different methods are proposed to detect Sybil attack. First one is detection using trust-based certificate and the second method is based on Received Signal Strength Indicator (RSSI).

 https://doi.org/10.37896/pd91.5/91567

ISSN: 0369-8963

Detection using Trust based certificate

Let consider the two nodes n_x and n_y . They belong to same cluster or from different cluster. In both the case, the genuineness of the nodes can be verified by the CH with the help of node specific CT send along with data packet being communicated. Since the CT is generated using the node location 'l' and node id, nodes from two different location cannot have the same certificate. Since the Certificates are generated dynamically in response to the request, the validity of the certificate can be determined based on the time period. If CT_{ri}^{t} is certificate sent by node 'i' at time 't', the CH retrieves the certificate (CT_{ai}^{t}) of node 'i' active for the time 't' from its database and compare it with the received certificate. If both are matching ie $CT_{ri}^{t} = CT_{ai}^{t}$, then the verification is successful. Else the CH concludes that message is received from Sybil node.

In a given time period, if two different packets with same node id with different certificates are being circulated, then the CH will verify the legitimacy of the nodes by comparing the received certificate with the certificate expected to be received during the give time lot. The node whose certificate does not belongs to specified time slot will be inferred as Sybil node.

$$RC(CT_a^{t1}) = RC(CT_b^{t2}) \;\&\&\; a = b \;\&\&\; t1 \neq t2$$

$$\Downarrow$$

$$\begin{cases} t1 \notin \; current\ time\ slot \;\Rightarrow\; node\ a\ is\ sybil\ node \\ t2 \notin \; current\ time\ slot \;\Rightarrow\; node\ b\ is\ sybil\ node \end{cases}$$

Evaluation of genuineness using certificate computed using the trust , location and node ID exhibits robustness in detecting the Sybil attack[11].

Detection using RSSI

Along with the certificate for recognizing Sybil attack, the arial distance between the neighboring nodes is also considered. A table data structure is maintained by each node. This stores the distance of all the neighboring nodes and used for tracking the range estimate.[12]. The very nature of wireless environment results in ranging error (RGE). While performing the distance verification, if two independent nodes are found with mutation in distance which is less than RGE, then the node performing the distance verification confirm the Sybil attack. The two nodes can be declared as Sybil node. Hence to eliminate the false positive rate in the detection of Sybil attack, strength of the received signal i.e., RSSI is considered as another vital parameter to reduce the false positive rate of Sybil attack detection [13]. In this method, whenever there is significant variation in RSSI is found during the time of node entering and leaving the network, it is considered to be the Sybil node. Algorithm for Sybil node detection based on RSSI is given below.

Algorithm 2

1. Let the number of node be 'M'
2. Construction of table which includes the distance factor of all the neighboring nodes
3. For each node n_i where $i \in \{1\ to\ M\}$ do the following steps
    a. The CH computes the trust value TF_i
    b. The CH generates CT_i using the parameter node id, nonce, trust factor TF_i and its current location 'l'.
    c. If $n_i \in M$ and $RC\left(CT_{n_i}^{t1}\right) = CT_{ai}^{t}$ $then$

        No Sybil attack

        Else

        Detection on Sybil node

 https://doi.org/10.37896/pd91.5/91567

ISSN: 0369-8963

a. If $n_i \in M$ and $RC(CT_{n_i}^{t1}) = RC\left(CT_{n_j}^{t2}\right)$ and $n_i = n_j$
   If $t1 = t2$
   No Sybil attack
   Else
   Detection on Sybil node
b. For each pair of nodes n_i and n_j where $i, j \in \{1\ to\ M\}$ and $neighbour(n_i) = n_j$
   a. n_i computes the distance between n_i and n_j
   b. If $dt(n_i, n_j) < RGE(mu)$ then
   If $RSSI(n_j) > TH$ and $RC(CT_j^{t1}) \neq CT_{aj}^{t}$ then
   n_j is designated as Sybil node

Simulation and results

The proposed scheme is simulated in NS2. The two parameter namely detection rate and false alarm rate are considered as vital for analyzing the performance the scheme.

Simulation scenario

For simulation, wireless sensor network with 20-200 nodes with 3-6 clusters deployed in the area of 100* 100 sqm is considered. The simulation parameter used in the evaluation of the proposed scheme is presented in table given below.

Parameter	**Value**
Number of nodes	20-200
Area	100 * 100 sqm
MAC	IEEE 801.11
Traffic type	CBR
Model of Antenna	Omni
Antenna Range	40 m

Table 4.1 Simulation Parameter

Rate of Detection

The accuracy of level of the proposed scheme is analyzed by measuring the rate of detection of Sybil attack for various number of Sybil attack nodes. The size of Sybil nodes is increased as 5, 10,15,20,25 for the network of size 150. Detection rate is computed using the equation given below.

$$Rate\ of\ Detction\ of\ attacks = (number\ of\ sybil\ nodes\ detected / total\ number\ of\ sybil\ nodes) * 100$$

The simulation results are given in fig2. The proposed system shows the high detection rate of 99%.

 https://doi.org/10.37896/pd91.5/91567

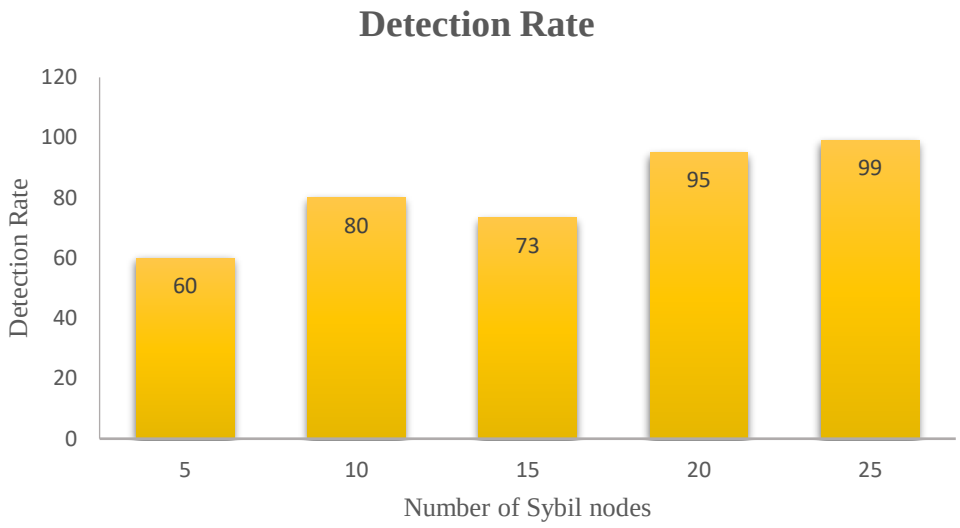

Fig 2 Sybil Attack Detection rate

False alarm rate

Another parameter which is considered vital for analyzing the performance of the proposed scheme is False Alarm rate. It is the measure of number of incorrect alarms or number of genuine nodes being detected as Sybil nodes. False Alarm rate is computed using the equation given below.

$$False\ Alarm\ rate = (number\ of\ false\ alarms/total\ number\ of\ \ nodes\ ) * 100$$

The simulation results given in fig 3 shows, the least rate of false alarm is 0.77.

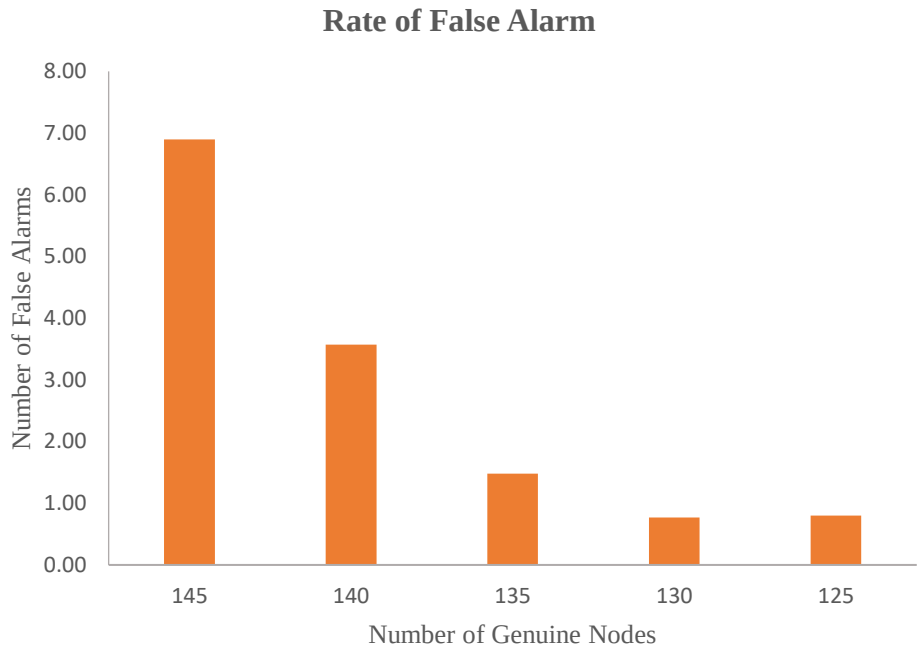

Fig 3 Rate of False Alarm

https://doi.org/10.37896/pd91.5/91567

Conclusion

We propose a lightweight framework for detecting Sybil attack in Wireless sensor network deployed using cluster topology. The framework is designed based on the certificate generated using the identity, trust, location and nonce. The accuracy level Sybil attack detection is improved by incorporating the RSSI based analysis. The proposed scheme is simulated in NS2. The simulation results supports that our proposed scheme exhibits high level of accuracy in the detection of Sybil attack.

References:

[1] Wen, M., Li, H., Zheng, Y.-F. and Chen, K.-F. 2008. Tdoa-based Sybil attack detection scheme for WSNs. Journal of Shanghai University English Edition 12(2): 66-70.

[2] Zhang, Y. Fan, K. F. Zhang, S. and Mo, W. AOA based trust evaluation scheme for Sybil attack detection in WSN Applied Research Computer, 27(2): 1847-1849, 2010.

[3] Mahdi Sadeghizadeha, " A lightweight intrusion detection system based on RSSI for Sybil attack detection in wireless sensor networks "Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 305-320. ISSN: 2008-6822 (electronic) http://dx.doi.org/10.22075/IJNAA.2022.5491

[4] Noor Alsaedi, Fazirulhisyam Hashim, A. Sali, Fakhrul Z. Rokhani , "Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS)", Computer Communications (2017), doi: 10.1016/j.comcom.2017.05.006

[5] Arthanareeswaran Angappan, · T. P. Saravanabava , P. Sakthivel , K. S. Vishvaksenan, " Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN", Journal of Ambient Intelligence and Humanized Computing (2020), https://doi.org /10.1007/s 12652-020-02276-5

[6] Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information" Expert Systems with Applications, Volume 42, Issue 21, 2015, Pages 7560-7572,ISSN 0957-4174, https://doi.org /10.1016/j.eswa.2015.05.057.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A survey on sensor networks, in IEEE Commu-nications Magazine, 40 (8) (2020) 102-114.

[8] M. G. Ball, B. Qela and S. Wesolkowski, A Review of the Use of Computational Intelligence in the Design of Military Surveillance Networks, in Recent Advances in Computational Intelligence in Defense and Security, (2015) 663-693.

[9] McGibney, A. et al. (2014). Wireless Sensor Networks for Building Monitoring Deployment Challenges, Tools and Experience. In: Langendoen, K., Hu, W., Ferrari, F., Zimmerling, M., Mottola, L. (eds) Real-World Wireless Sensor Networks. Lecture Notes in Electrical Engineering, vol 281. Springer, Cham. https://doi.org/10.1007/978-3-319-03071-5_24

[10] Borz, I., Palade, T., Puschita, E., Dolea, P., Pastrav, A. (2022). Wireless Sensor Networks for Healthcare Monitoring. In: Vlad, S., Roman, N.M. (eds) 7th International Conference on Advancements of Medicine and Health Care through Technology. MEDITECH 2020. IFMBE Proceedings, vol 88. Springer, Cham. https://doi.org/10.1007/978-3-030-93564-1_26

[11] R. Amuthavalli and R. S. Bhuvaneswaran, Genetic algorithm enabled prevention of Sybil attacks for LEACH- E, Modern Applied Science 9(9), pp. 41–49 (2015).

[12] P. Sarigiannidis, E. karapistoli and A. A. Economides, Detecting Sybil attacks in Wireless Sensor Networks using UWB ranging based information, Elsevier- Expert System Applications 42(21), pp. 7560-7572 (2015).

[13] R. Vinothkumar, P. Ramesh, H. A. Rauf, "Cluster based enhanced Sybil attack detection in MANET through integration of RSSI and CRL," IEEE Xplore digital library, December 2014.

[14] Douceur JR (2002) The Sybil attack. In: International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, pp 251–260

[15] Demirbas M, Youngwhan S (2006) An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In: 2006 international symposium on a world of wireless, mobile and multimedia networks (WoWMoM'06). IEEE

[16] Vinodha,D , Mary Anita, EA 2021, 'Discrete Integrity Assuring Slice-Based Secured Data Aggregation Scheme for Wireless Sensor Network (DIA-SSDAS)', Wireless Communications and Mobile Computing, vol. (2021) Article ID 8824220, https://doi.org/10.1155 /2021/ 8824220, ISSN: 1530-8669.

[17].Vinodha, D, Mary Anita, EA 2021, 'A novel multi functional multi parameter concealed cluster based data aggregation scheme for wireless sensor networks (NMFMP-CDA)', Wireless Networks, Springer vol. 27, no. 2, pp. 1111-1128 (2021) https://doi.org/10.1007/s11276-020-. 02499-6. ISSN:1022-0038.

[18] E.A. Mary Anita, "Sybil Secure Architecture for Multicast Routing Protocols for MANETs", Communications in Computer and Information Science, Springer-Verlag GmbH Berlin Heidelberg, Volume 190, 2011, pp 111-118.