J Electr Eng Technol.2018; 13(6): 2447-2455
http://doi.org/10.5370/JEET.2018.13.6.2447

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

SEC Approach for Detecting Node Replication Attacks in Static Wireless Sensor Networks

L. Sujihelen†, C. Jayakumar* and C. Senthilsingh**

Abstract – Security is more important in many sensor applications. The node replication attack is a major issue on sensor networks. The replicated node can capture all node details. Node Replication attacks use its secret cryptographic key to successfully produce the networks with clone nodes and also it creates duplicate nodes to build up various attacks. The replication attacks will affect in routing, more energy consumption, packet loss, misbehavior detection, etc. In this paper, a Secure-Efficient Centralized approach is proposed for detecting a Node Replication Attacks in Wireless Sensor Networks for Static Networks. The proposed system easily detects the replication attacks in an effective manner. In this approach Secure Cluster Election is used to prevent from node replication attack and Secure Efficient Centralized Approach is used to detect if any replicated node present in the network. When comparing with the existing approach the detection ratio, energy consumption performs better.

Keywords: SEC-Secure-Efficient for centralized, NAK-Novel Alphanumeric Key, Node replication attacks, Paillier method, Secure CLUSTER Election

1. Introduction

The Wireless Sensor Network has a collection of sensor nodes that are equipped with a transceiver, micro controller, etc [1, 15, 19]. These sensor nodes are deployed in the unattended environment to fulfill the different applications such as military and civil applications [18]. Each sensor nodes have limited storage capacity, low energy, less power and less security [1, 17]. Due to less security, it is prone to different kind of attacks. Among the most vicious attacks is the replication attack, which has also been declared as a unique security threat. This is a very serious threat to distinguish due to the similarity in the features between the replicated and the original node. Any internal node is captured by unauthorized persons and the observed features [16] are replicated into their own new node which is later launched into a dynamic working WSN to make it work like a typical legitimate node. It was almost impossible to find these nodes out when all the applications were going down due to reasons unknown earlier. Sensor nodes are not tamper-proof, the adversary capture node information are all stored in network communications [5, 31].

To do the malicious activities the adversary may replicate the captured sensor nodes and placed it in the network. This type of attack is called as node replication attacks [11, 6, 22]. This clone node misbehaves in the network. It affects the major parts of the network such as routing, packet loss, etc. To detect the replicated node a Secure Efficient Approach is proposed. This proposed system works for preventing and detecting the replicated node in the sensor network. The Secure Cluster Election is used to elect the cluster head and secure the nodes with a random number. The SEC approach is used to detect the replicated node at a random time in the sensor network. The SEC verification will verify the clone node exactly. In this proposed system, it detects the replicated node quickly and 100% accuracy.

In this paper, SEC approach is proposed to detect the replicated node in centralized static wireless sensor networks. The organization of this paper is: section 1: Introduction; section 2: Related works; section 3: Proposed system; section 4: Simulation of SEC; section 5: Conclusion.

2. Related Work

To detect the clone nodes more methods are proposed. A detection protocol is used to detect the clone nodes that counts the number of keys used by the node [3]. If the number of keys is more, the detection technique is used [28]. A Bloom Filter and random key predistribution techniques are used in this method. The detection accuracy is poor. If the key size is very small, more replica nodes are found [34].

A SET approach is proposed for detecting replicated node in centralized static wireless sensor network. The

† Corresponding Author: Dept. of Computer Science and Engineering, Sathyabama Institute of Science & Technology, Chennai, India. (sujihelen@gmail.com)
* Dept. of Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India. (cjayakumar2007@gmail.com)
** Dept. of Electronics & Communication Engineering, Adhi College of Engineering, Chennai, India. (senthilsingh@gmail.com)
Received: February 16, 2017; Accepted: January 2, 2018

network is randomly divided into subsets. The clone nodes are detected by the intersection of the two subtrees [9]. This method [2] reduces the detection overhead, but it misuses to revoke the genuine node [27]. In distance traveled sliding window [2] approach is used to detect the replicated node in Mobile WSN and it uses only location criteria for detecting the clone node. If the clone node has the same location, then it is assigned as a genuine node [35, 36].

In CSI method, all nodes broadcast the data to its one-hop neighbors [13]. The clone node is detected based upon the sensed data [4]. If the reading is less for clone node, this method fails to detect the node replication attack.

A detection technique is proposed by computing the fingerprint through as-disjunct code. Each node stores the fingerprint of all neighbors [12, 7, 29]. However, computation of fingerprint and managing the neighbor's information has high storage overhead.

A Bloom Filter and Hash function are used for Detecting Node Replication Attack [14, 20]. If two nodes have the common id, then the bloom filter technique is applied to check replicas. Detecting is based only upon node id that does not detect the replication node accurately [26, 35].

When a node has to transmit a location claim [10, 23], it will first check for clone and then forwards the location claim to the node nearest to the global destination [30, 38]. In this approach all the intermediate nodes in the route start working as a temporary witness node. The proposed system overcomes the issues of existing work.

3. Proposed System

In this proposed system, SCE(Secure Cluster Election) and SEC (Secure, Efficient, Centralized) approach is introduced. The Secure Cluster Election is to elect the cluster head and secure by using a paillier method to prevent the clone node. The SEC concern is to notice the replicated node in centralized static WSN. The location of nodes cannot change static WSN.

Detecting the replicated node is considered to be a difficult task. In this proposed system the detection process is carried out by a central authority or Cluster Head shown. Each cluster head communicates Base Station (BS).

3.1 Network model

It consists of N nodes that are deployed in a m x n terrain. The nodes are deployed on the terrain [33]. Each node information such as Node id(N), Energy(E), Location id (L) are stored in the BS. During deployment the security keys are given by BS to each node. The node is deployed with the following fields: node id, common energy level for all the nodes (E), location id (L), Random number(R) is generated by BS and given to the cluster head during cluster formation[8], private key (K) is taken from the key pool for communication, neighbor node id (N), fixed data size for each node (S). The node information is shown in Fig. 1.

Node id	Loc. Id	Random number	Keys	Energy	Neighbor node	Fixed data size for each node

Fig. 1. Fields for each node

3.2 Secure cluster head selection

In this proposed Secure Cluster head Selection method, the base station is taking the charge of electing all the cluster heads [32, 37]. When a node joins the base station, the base station stores the information about that node. The cluster head election takes place when the energy level of the cluster head exceeds the limit(α). The cluster head is elected, based upon the different criteria.

a) The cluster is elected upon the node which is more proximate to the Base station. The distance between the node and the BS is calculated. The distance is calculated by using

$$D=\sqrt{\sum_{i=1}^{N}(xi-ci)^2} \quad (1)$$

$$Ci=\frac{1}{mi}\sum_{x\in ci} x \quad (2)$$

The distance is calculated for each node. Select the node which has a shorter distance.

b) Check the energy efficiency of the node which has a shorter distance [21].

$$E1 = T(d) + R \quad (3)$$

In the above, R is the energy required to receive the packet, T is energy spent by the transmitter and d is the distance. The power consumption [25] in transmitting (T) and receiving (R) the message (m), a distance d can be computed as

$$T(m,d)=E\_elec \times m + \varepsilon\_(amp)\times m\times d^2 \quad (4)$$

$$R(m)=E\_elec\times m \quad (5)$$

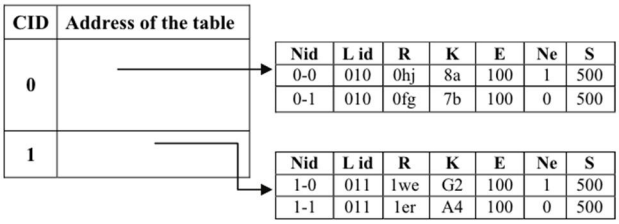
While transmitting and receiving the events (E1) each and every time the energy is reduced from the previous energy E.

The structure of the cluster head and the nodes in the network details are shown in fig. 2

$$E = E - E1 \quad (6)$$

From the nearest nodes and the nodes that have high energy is filtered

c) Select the node which is not selected as cluster head from the filter node. Once the cluster head is elected, the cluster head sends a message (Bmsg) to all the nodes which are nearer to the cluster head.



CID	Address of the table
0	
1	

Nid	L id	R	K	E	Ne	S
0-0	010	0hj	8a	100	1	500
0-1	010	0fg	7b	100	0	500

Nid	L id	R	K	E	Ne	S
1-0	011	1we	G2	100	1	500
1-1	011	1er	A4	100	0	500

Fig. 2. Cluster head structure

Algorithm to secure Cluster Head using Paillier Method

1. Choose two prime numbers randomly and assign as A,B, S1=0.
2. Find **GCD**(A*B,(A-1)(B-1)) and **Compute** n=A*B
3. **Calculate** λ=lcm(A-1, B-1)
4. Select any random integer s, where s∈Z*, where Z is an integer number.
5. Choose any random number and assign as m and r, where m, r∈Z*
6. **Compute** $C=s^m.r^n(\text{mod } n^2)$
7. **Compute**, $m=L(C^{\lambda}(\text{mod } n^2)).\mu(\text{mod } n)$
   Where, $\mu=(L(g^{\lambda}(\text{mod } n^2)))^{-1}(\text{mod } n)$
   $L(\mu)=\frac{\mu-1}{n}$
8. **Until** the m value is received, the below step is repeated.

```
if (m!=0)
  begin
        Y=m%10
        S1=s1+y
        M=m/10
  End
    Cluster id=s1.
     End
```

$$Bm = (Chid, Bmsg) \quad (7)$$

After selecting the cluster head the BS will secure the cluster head using Paillier method of generating the random number (R).Cluster Head id is generated by BS, by using the paillier method. S1 is generated by BS and given to the Cluster head as cluster id. Each cluster member is assigned a random number by combining s_1, m with Rand (0, ALPHSIZE-1). Assume S1=6, m=124, and the alphanumeric, random number is 00CB, and then the cluster member random number is 612400CB. The Secure clustering Algorithm prevents the replicated node in the sensor network with a random number. During cluster election, the base station distributes the random number to all the nodes through cluster head. The random number is not constant. It changes during the cluster election. If a new node tries to enter into the network, then the random number and key should be verified by the base station. If the verification fails, then the node disconnects from the network.

3.3 SEC approach

SEC algorithm is used to find the exact replicated node. If it is a replicated node, it terminates its communication link. The Base Station takes the responsibility of detecting the replicated node. The overview of the SEC approach is shown in the Fig. 3. In this method a Novel Alphanumeric Key (K) that is verified while node-to-node communication takes place in the WSN. A key is generated in every communicating node that is meant to reply with a route to any node. If a route reply is received without this key, the communication to that node will be instantly terminated. Novel Alphanumeric Key (K) is generated by the equation below, where m = modulus (m > 0), a = multiplier (0 < a < m), X_0 = starting value ($0 \le X_0 < m$).

Algorithm to Secure Cluster Selection

1. **Assign** node id for all nodes by BS.
2. Compute number of Cluster heads in network
   $CH=\frac{N}{\text{limit nodes}}$
3. **Repeat until** i=1 to N
   begin
   Assign R=a[i].e, Q=a[1].d. **Distance** is calculated as $D=\sqrt{\sum_{i=1}^{N}(xi-ci)^2}$
   If (a[i].d< Q) then
   begin
   assign Q=a[i].d, **Compute** the energy E = T(d)+ R
   If (a[i].E>R) then
   begin
   assign R=a[i].E,
   Select the a as the Cluster head.
   End
   End
4. **Compute** the random number(s) by paillier method.
5. **Send** BS(s,C,msg)
6. **Ack** C(BS ,msg)
7. **Send** C(s-nodeid,N,Msg)
8. **Join**(Chid,msg)
9. Cluster validate with BS
10. **Ack** N(CH, msg)
11. After validation Accept(nodeid, msg)
12. **join**(Chid,msg)
    End

$$x_{n+1} = [a * x_n] \,(\text{mod m}) \quad (8)$$

3.3.1 Node Detection

To detect the replicated node three criteria are used: i) The nodes are deployed as a static. Each node location id is stored in the neighbor node. While communicating from one node to another node the neighbor node [14] automatically monitors their location id, node id and the distance between the neighbor node (d_{ij}). If the location id, node id or the distance does not match, then the neighbor node reports to the cluster head. At this stage the SEC algorithm is used by BS to identify the replicated node. ii) If the node is replicated and placed in some other cluster, then the replicated node is found by the neighbor node and report it to the cluster head by verifying the node id,

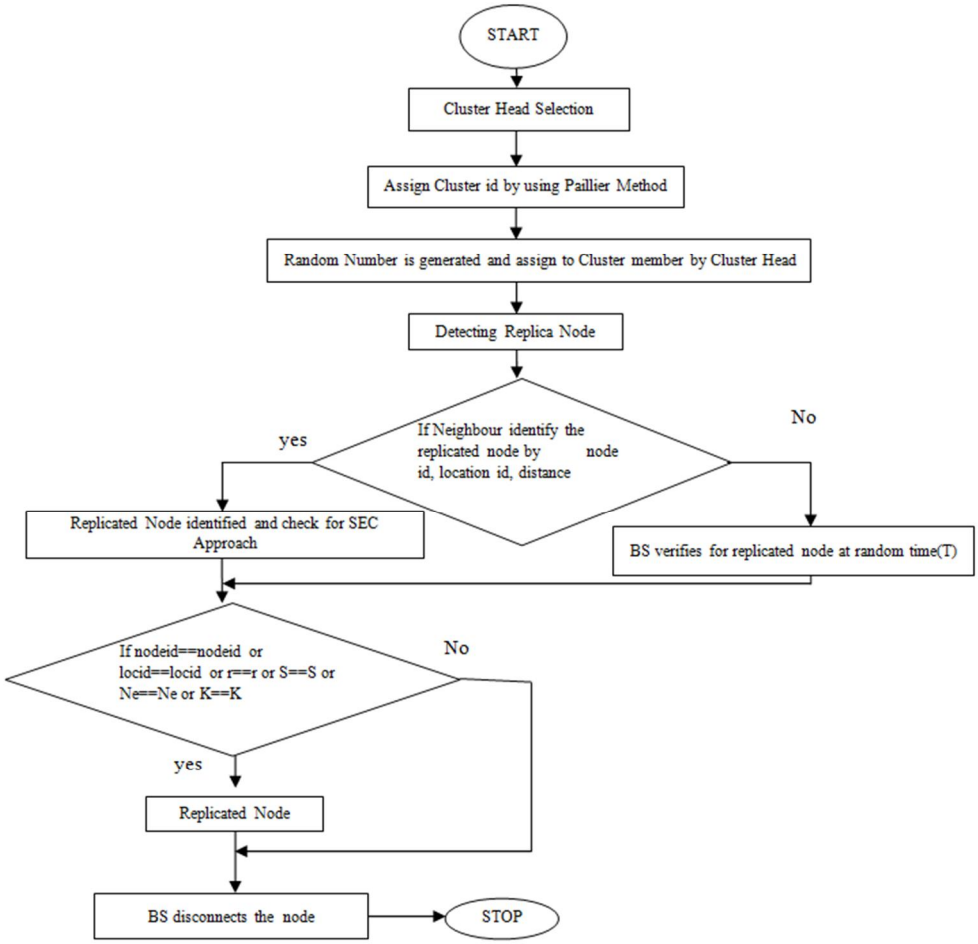


Fig. 3. Overview of SEC Approach

Algorithm: (SEC Approach-Secure Eficient for Centralized Approach)

```
1. Assign BS, CH, ./*BS-Base Station, CH-
   Cluster Head, N-Total number of Nodes*/
2. For(i=1 to CH)
   Begin
   2.1 For (j= 1 to n) nodes present in CH
     Begin
      If (CH (nodeid) = = nodeid)
            /* node id already exist*/
       If (CH (nodeid (locid))!=Locid)
            /* Check for Location*/
       If (CH (nodeid (Rand)! = Rand)
          /*check for Random number*/
       If (CH (nodeid (energy))! =nodeid
         (energy)  /* Check for energy */
       If (CH (nodeid (datasize))) >  fixed
          size)  /* Check for data size*/
           Assign as Clone Node
         Else
             Not a clone Node
       End
   End
```

location id and the distance. The misbehavior node is identified and reported to the cluster head. The cluster head reports it to the BS and the replicated node is removed from the link. iii) At each time (T) the randomly selected node should report their random number, location id and node id to BS through cluster head [24]. BS identifies the replicated node by SEC approach.

4. Detecting Replicas

It is assumed that A is an attacker node. The probability for one attacker node present in the network is

$$P(A) = 1\text{-}P(\hat{A}). \quad (9)$$

If the probability for no replicated node is found in the network, then the probability is

$$P(A) = P(A) / P(S) \quad (10)$$

Where A is the attacker node and S is the path or network. Suppose A is the attacker node and S is the collection of nodes present in the cluster, then the number of replicated nodes present in the cluster are

$$P(A) = \frac{n(A)}{n(S)} \quad (11)$$

4.1 Detecting the replicas by SEC approach

It is considered that 50 nodes are there in the WSN. The nodes are randomly chosen and the conditions are applied such as node id, Location id, Energy Level, Random Key, Data Limit. Assume B1 as Node id, Location id as B2, Energy Level as B3, Random Key as B4 and Data Limit as B5. It is considered that the 50 nodes in the WSN as A. For the condition node id B1, the replicated nodes are found to be

$$P\left(\frac{A}{Bl}\right) = \frac{P(A)P\left(\frac{Bl}{A}\right)}{P(Bl)} \quad (12)$$

It is assumed that, after applying this condition 10 nodes are filtered such as A1, A20, A23, A26, A29, A30, A35, A40, A45, A49. Let it be assumed that the filtered node as C={A1,A20,A23,A26,A29,A30,A35,A40,A45,A49}. The Location id B2, the probability are

$$P(C/B2) = \frac{P(C)P(^{B2}/_{C})}{P(B2)} \quad (13)$$

The replicated nodes filtered are A1, A23, A29, A30, A35, A40, A45. All the filtered nodes are considered as D. The Energy Level is B3 and the following condition is applied.

After applying this condition assume that the replicated nodes filtered is

$$P(D/B3) = \frac{P(D)P(^{B3}/_{D})}{P(B3)} \quad (14)$$

A1, A29, A30, A35, A40, A45. All the filtered nodes are considered as E. It is considered that the Random Key is B4 and the condition given below is applied

$$P(E/B4) = \frac{P(E)P(^{B4}/_{E})}{P(B4)} \quad (15)$$

After applying this condition it is assumed that the replicated nodes filtered are A1,A29,A30,A35,A40. All the filtered nodes are considered as F. The Data Limit B5 is taken into consideration and the condition given below is applied. After applying this condition it is assumed that the replicated nodes filtered are A1, A30, A35, A40. Now the exact replicated node is detected by using this proposed SEC approach. The table 1 shows the detected clone nodes.

$$P(F/B5) = \frac{P(F)P(^{B5}/_{F})}{P(B5)} \quad (16)$$

Table 1. Detection rates by SEC Approach

No.of Nodes	No.of Cluster	Maximum clone Nodes	No. of Clone Nodes Detected by SEC Approach	Correctly Detected nodes
100	1	7	7	7/7
200	1	11	11	11/11
500	3	15	15	15/15
600	3	17	17	17/17
1000	5	20	20	20/20
2000	10	25	25	25/25

5. Performance Evaluation

Consider the network size is n and the cluster head is c. Each cluster head ends message to the nodes as (t-1) messages. The proposed algorithm is compared with the existing algorithm [8]. The hierarchical node algorithm using bloom filter [8] has the communication overhead as 2(t-1) messages. The communication cost for the SEC approach is $\Theta(t)$. When compared with the hierarchical node algorithm the communication cost for the SEC approach is lesser. For the bloom filter, it occupies 800 bits. But in the SEC approach it occupies lesser than 200 bits for storing the node id and location id. So memory cost is less in SEC approach.

5.1 Simulation Results

In the experimental setup the characteristics of the node and its performance are analyzed using the proposed SEC approach. The SEC approach is tested by the NS-2 simulator. Network simulator is a very convenient and effective tool for assessing the security systems and has been extensively used by the researchers to prove numerous concepts before. The simulation parameters are shown in the table 2. Therefore,

NS-2 is used to perform simulations for SEC approach. Table 2 shows the parameters which are used for the construction of the network.

During the simulation time, the statistics are collected. The different performance measures used in the evaluation are given below.

5.2 Detection accuracy

It is used to represent the false positive ratio and false

Table 2. Simulation parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	100 s
Number of nodes	50
MAC type	802.15.4
Traffic model	CBR
Simulation Area	1100×700
Transmission range	250m
Network interface Type	WirelessPhy
Initial Energy	10 J

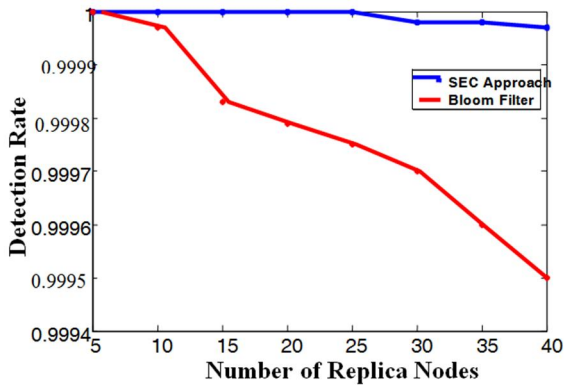


Fig. 4. Detection accuracy

negative ratio of the algorithm. The ratios of falsely considering a genuine node as a replica and falsely considering a replica as a genuine node, respectively. The detection accuracy is calculated as

False Detectionrate=

$$\frac{\text{No.of Replica Nodes} - \text{No. of Replica Node Identified}}{\text{No. of Replica Nodes}} * 100 \quad (17)$$

As shown in the Fig. 4, the detection accuracy can be easily observed. It shows that the detection accuracy of the replica node is not lower than 99.9% that is achievable. This method detects the exact replicated node.

5.3. Detection time

It is assumed that there are 3 replica nodes are present in the network. While the replica node is deployed the neighbor node easily identifies the node by their misbehavior. If the neighbor node is not detecting replica node, then at a random time a group of node information is sent to the BS which verifies its misbehavior and detects the replica node. The replicated node is identified automatically, once the replica node is deployed. The detection time delay rate is very less when compared to the other existing algorithms.

5.4. Average delay

The average delay is defined as the time difference between the current packets received and the previous packets received. The time is measured by the following equation.

$$\text{Delay} = \frac{\sum_0^n \text{packet send time} - \text{packet received Time}}{\text{Time}} \quad (18)$$

Fig. 5 shows that the delay value is lower for the proposed scheme of static than the existing Bloom Filter algorithm [8].

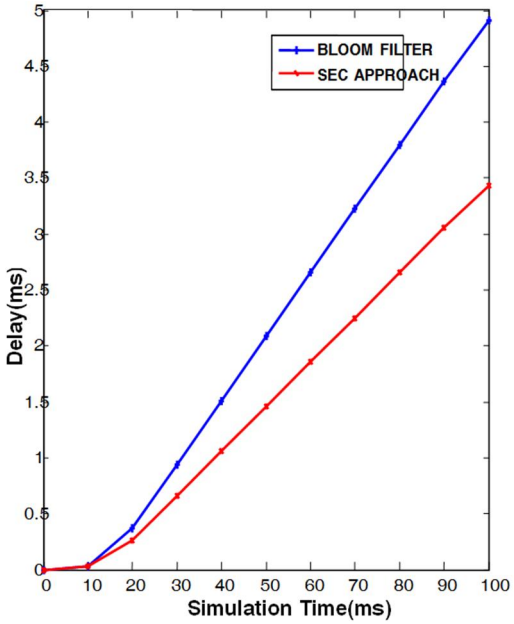


Fig. 5. Average delay

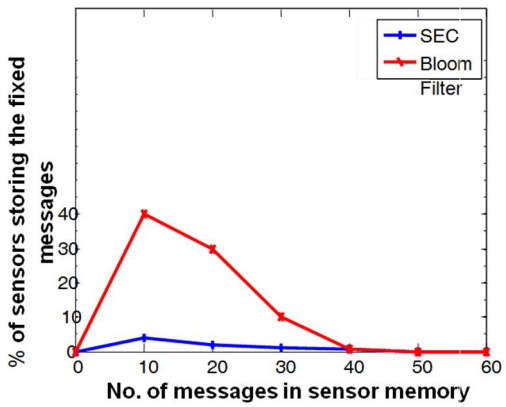


Fig. 6. Storage overhead

5.5 Computation and storage overhead

The computation and storage overhead calculated as the average number of verification operations and less storage in sensor node. The neighboring node verifies the nearest node to communicate between the two nodes. If any misbehavior is found, it is informed to BS. When compared with the existing algorithm the storage is very less shown in Fig. 6. BS verifies the misbehavior of the node and assign the node as a clone node or not.

5.6. Residual energy

A measure of the residual energy gives the rate at which energy is consumed by the network operations. Fig. 7 shows that the residual energy of the network is better for the proposed scheme for static when compared with the existing Bloom Filter [8].

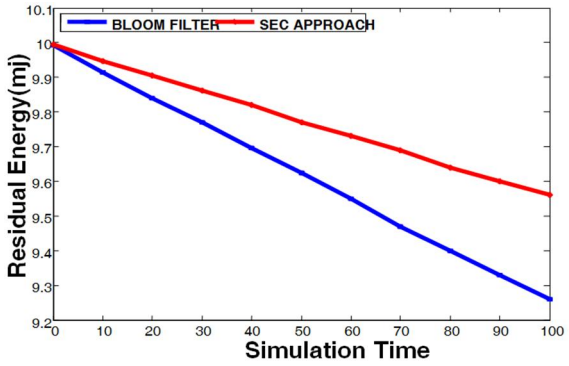


Fig. 7. Residual energy

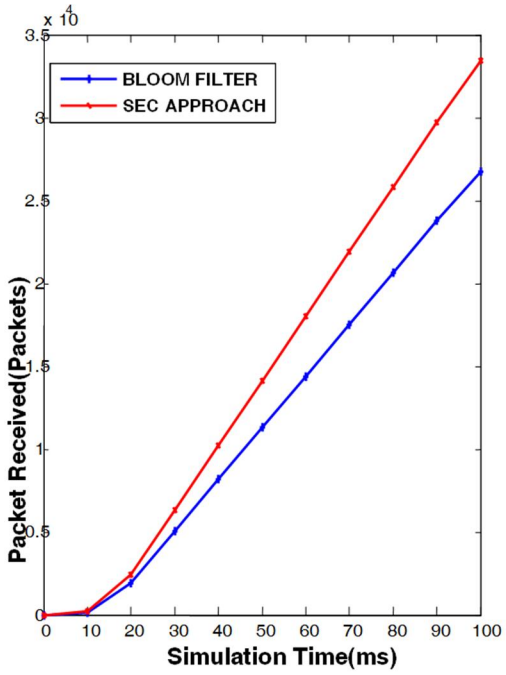


Fig. 8. Packets received

5.7 Packets Received

The total number of packets received in the SEC approach and the Bloom Filter [8] are plotted in Fig. 8. In Bloom Filter [8] approach, messages for each and every link establishment causes greater overhead and packet loss. Therefore SEC performs better than the existing approach [8] as observed in Fig. 8 and Fig.

6. Conclusion

This paper proposed a method to detect the replicated node in Static networks. The novel Secure, Efficient Centralized (SEC) approach used to detect the exact replicated node in Static WSN. Simulation analysis has been performed for SEC under static conditions. From the simulation results, it can be concluded that this method

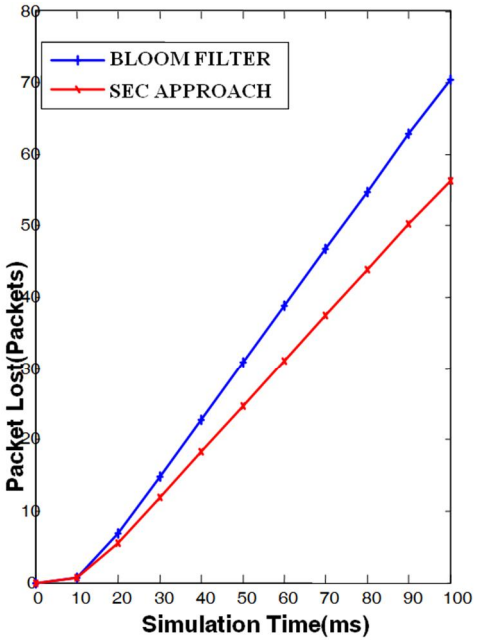


Fig. 9. Packets lost

serves to be one of the most efficient methods to detect the replicated node from the network.

This algorithm works in a centralized static approach. In future work, the proposed work is extended for the centralized mobile approach and distributed static and mobile approach.

References

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. "A survey on sensor networks," *IEEE Communication*, vol. 40, no. 8, pp. 102-114, 2002.

[2] Alekha Kumar Mishra, Asis Kumar Tripathy, Arun Kumar, and Ashok Kumar Turuk, "A Replica Detection Scheme Based on the Deviation in Distance Traveled Sliding Window for Wireless Sensor Networks," Wireless Communications and Mobile Computing, 2017.

[3] Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, KandemirMT, "On the detection of clones in sensor networks using random key predistribution," *IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews*, vol. 37, no. 6, pp. 1246-1258, 2007.

[4] L. Sujihelen, C. Jayakumar, C. Senthilsingh, "Detecting Node Replication Attacks in Wireless Sensor Networks Survey," *Indian Journal of Science and Technology,* 2015, vol. 8, no. 16, 2015.

[5] Vijayan K, Raaza A, "A novel cluster arrangement energy efficient routing protocol for wireless sensor networks," *Indian Journal of Science and Technology*, vol. 9, no. 2, 2016.

[6] Wang Y, Attebury G, Ramamurthy B, "A survey of security issues in wireless sensor networks," *IEEE Communications Survey and Tutorials*, vol. 8, pp. 1-23, 2006.

[7] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, Yang Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, 2013.

[8] Znaidi Wassim, Marine Minier, Stéphane Ubéda, "Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, 2013.

[9] Choi H, Zhu S, La Porta TF, "SET: Detecting node clones in sensor networks," *Third International Conference on Security and Privacy in Communications Networks*, pp. 17-21, 2007.

[10] Ko LC, Chen HY, Lin GR, "A neighbor-based detection scheme for wireless sensor networks against node replications attacks," *IEEE International Conference on Ultra Modern Telecommunications and Workshop*, pp. 1-6, 2009.

[11] Manjula V., Chellappan C, "The Replication Attack in Wireless Sensor Networks: Analysis and Defenses," *Advances in Networks and Communications. Communications in Computer and Information Science*, vol. 132, 2011.

[12] Xing K, Cheng X, Liu F, Du DHC, "Real-time detection of clone attacks in wireless sensor networks," *International Conference on Distributed Computing Systems*, pp. 3-10, 2008.

[13] Yu CM, Lu CS, Kuo SY, "CSI: Compressed sensing-based clone identification in sensor networks," *IEEE International Conference on Pervasive Computing and Communications*, vol. 290, 2012.

[14] Znaidi M, Ubeda MS, "Hierarchical node replication attacks detection in wireless sensors networks," *Proceedings of IEEE Personal, Indoor and Mobile Radio Communications*, vol. 82, 2009.

[15] Y. Zhang & P. Kitsos, "Security in RFID and Sensor Networks," *CRC Press, Taylor & Francis Group, chapter 14*, pp. 293-320, 2009.

[16] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," *in Proceedings of the IEEE Symposium on Security and Privacy*, pp. 49-63, May 2005.

[17] Pantazis, N.A., Nikolidakis, S.A. and Vergados, D.D., "Energy-efficient routing protocols in wireless sensor networks: A survey" *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 551-591, 2013.

[18] B. Rashid, and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: a survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192-219, 2016.

[19] Umer, T., Amjad, M., Afzal, M.K. and Aslam, M., "Hybrid Rapid Response Routing Approach for Delay-Sensitive Data in Hospital Body Area Sensor Network," *In Proceedings of the 7th International Conference on Computing Communication and Networking Technologies*, 2016

[20] Xiaodong Song, Xiang Wang, "New Agent -based Proactive Migration Method and System for Big Data Environment(BDE)," *Engineering Computations*, vol. 32 (8), pp. 2443-2466, 2015.

[21] Degan Zhang, Guang Li, Ke Zheng,"An energy-balanced routing method based on forward aware factor for Wireless Sensor Network," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 766-773, 2014.

[22] Degan Zhang, Xiang Wang, Xiaodong Song, "A Novel Approach to Mapped Correlation of for RFID Anti-collision," *IEEE Transactions on Services Computing*, vol. 7, no. 4, pp. 741-748, 2014.

[23] Yanping Liang, "A kind of novel method of service aware computing for uncertain mobile applications," *Mathematical and Computer Modeling*, vol. 57, no. 3-4, pp. 344-356, 2013.

[24] Ke Zheng, Ting Zhang,"A Novel Multicast Routing Method with Minimum Transmission for WSN of Cloud Computing Service," *Soft Computing*, vol. 19, 7, pp. 1817-1827, 2015.

[25] Xiaodan Zhang, "Design and implementation of embedded uninterruptible power supply system (EUPSS) for webbased mobile application," *Enterprise Information Systems*, vol. 6, no. 4, pp. 473-489, 2012

[26] Degan Zhang, "A new approach and system for attentive mobile learning based on seamless migration," *Applied Intelligence*, vol. 36, no. 1, pp. 75-89, 2012.

[27] Ke Zheng, Dexin Zhao, "Novel Quick Start (QS) Method for Optimization of TCP," *Wireless Networks*, vol. 22, no. 1, pp. 211-222, 2016.

[28] Yannan Zhu, "A new constructing approach for a weighted topology of wireless sensor networks based on local world theory for the Internet of Things (IOT)," *Computers & Mathematics with Applications*, vol. 64, no. 5, pp. 1044-1055, 2012.

[29] Xiang Wang, Xiaodong Song, "New Medical Image Fusion Approach with Coding Based on SCD in Wireless Sensor Network," *Journal of Electrical Engineering & Technology*, vol. 10, no. 6, pp. 2384-2392, 2015.

[30] Song X D, Wang X, "Extended AODV Routing Method Based on Distributed Minimum Transmission (DMT) for WSN," *International Journal of Electronics and Communications*, vol. 69, no. 1, pp. 371-381, 2015

[31] X J Kang, "A novel image denoising method based on spherical coordinates system," *EURASIP Journal on Advances in Signal Processing*, vol. 10, pp. 1-10 2012.

[32] Xiang Wang, Xiaodong Song, "New Clustering

Routing Method Based on PECE for WSN," *EURASIP Journal on Wireless Communications and Networking*, vol. 162, pp. 1-13, 2015.
[33] Zhao C P, "A new medium access control protocol based on perceived data reliability and spatial correlation in wireless sensor network," *Computers & Electrical Engineering*, vol. 38, no. 3, pp. 694-702, 2012.
[34] Li W B, "Novel Fusion Computing Method for BioMedical Image of WSN Based on Spherical Coordinate," *Journal of Vibro engineering*, vol. 18, no. 1, pp. 522-538, 2016.
[35] Ma Z, "Shadow Detection of Moving Objects Based on Multisource Information in Internet of Things," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 29, no. 3, pp. 649-661, 2017.
[36] Ma Z, "A Novel Compressive Sensing Method Based on SVD Sparse Random Measurement Matrix in Wireless Sensor Network," *Engineering Computations*, vol. 33, no. 8, pp. 2448-2462, 2016.
[37] Si Liu, Ting Zhang, "Novel Unequal Clustering Routing Protocol Considering Energy Balancing Based on Network Partition & Distance for Mobile Education," *Journal of Network and Computer Applications*, vol. 88, no. 15, pp. 1-9, 2017
[38] Zhou S, Yameng Tang, "A low duty cycle efficient MAC protocol based on self adaption and predictive strategy," *Mobile Networks & Applications*, 2017.

L. Sujihelen received the M.E. degree in Computer Science and Engineering. Currently doing Ph.D., in Computer Science & Engineering, Sathyabama University, Chennai, India. Her research interest includes Image processing, Wireless Sensor Networks.

C. Jayakumar received the M.E. Degree in Computer Science & Engineering from Anna University. Completed his Ph.D., in Anna University. Currently working as a Professor in Sri Venkateswara College of Engineering. His area of interest includes WSN, Data Mining.

C. Senthilsingh received the M.E. Degree in VLSI. Completed his Ph.D., in Anna University. Currently working as a Professor in Adhi College of Engineering. His area of interest includes Image Processing, WSN.