IJCSC 0973-7391 Volume 7 • Number 1 Sept 2015 - March 2016 pp.50-58 available online at www.csjournalss.com

Detection of Node Replication Attack Using XED and EDD algorithms in Wireless Sensor Networks

Manisha R. Deore[1], R. V. Patil[2]

[1]Master Student Computer Science & Engineering, SSVPS'S B.S.Deore College of Engineering, India
[2]Associate Professor, Computer Science & Engineering, SSVPS'S B.S.Deore College of Engineering, India
[1]deore.manisha28@gmail.com; [2] patil.rajendra@ssvps.com

Abstract: In these days, randomly moving sensor networks are more commonly used for building up a application in many areas like industrial, environmental, and medical and so on. There are some disadvantages of this network over the WSN, this network faces the problem like security attack and they create clones of the nodes. They face this problem because of their dynamic nature. There are some solutions for noticing the attack of node replication. Thus we deal with the challenging problem of node replication detection. Although defending against node replication attacks requires immediate attention, detecting node replication attacks in static networks, only a few solutions in mobile networks have been presented. Therefore, two localized algorithms are proposed to detect node replication attacks in wireless sensor networks. The advantages of our proposed algorithms include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance.

Keywords: Replication attack, security, wireless sensor networks, localized detection.

1. INTRODUCTION

A wireless sensor network (WSN) in simplest way can be defined as a network of possibly low-size and low-complex devices that denoted as nodes that can sense the environment and also communicate the information gathered from the different monitored field through wireless links; the data between the nodes is forwarded, possibly via multiple hops , to a sink that can use it locally, or it is also connected to other networks (e.g., the Internet) through a gateway.

- The nodes in the network can be stationary or moving.
- They can be aware of their location or not.
- They can be homogeneous or not.

Wireless Sensor Networks are composed of individual embedded systems that are capable of:

- Interacting with their environment through various sensors.
- Processing information locally.
- Communicating this information wirelessly with their neighbours[3]

WSN consist of many small sensor nodes. And these nodes vary from several hundreds to thousands. These sensor nodes work in the network in a collaborative manner to achieve a common goal. Sensor network is mainly used for interaction between computer system and there environment. The purpose of these autonomous sensor nodes to monitor different physical or environmental conditions in the network, such as temperature, pressure, sound etc. and also pass their data through the network to a destination location. Figure 1 shows a typical simple wireless sensor network. The different modern networks are bi-directional; also consist of control of sensor activity. The development of wireless sensor networks was mainly motivated by military purpose applications such as battlefield surveillance; today such types of networks are used in many industrial and consumer applications, like industrial process monitoring and control, machine health monitoring, and so on. Basic components of WSN nodes are Sensors, memory, GPS, processor, Radio transceiver and power source and major components of WSN are sensor node and base station. Sensor nodes in the network are known as sensing cells and base station as brain of wireless sensor network. WSN consists of mainly distributed autonomous sensor nodes to monitor physical or environmental conditions. The sensor node vary in their size .They may be as large as shoebox or may be size of grain of dust. The cost of sensor nodes vary, it may ranges from a few to hundreds or thousands of dollars, it is solely depends on the complexity of the individual sensor nodes.

WSN is mainly consisting of two types that are Stationary and Mobile WSN. In stationary WSN sensor nodes are stationary while in mobile WSN nodes can move and after deployment can interact with physical environment. Depending on the type of WSN attacks can vary [4].

DOI: 10.090592/IJCSC.2016.007

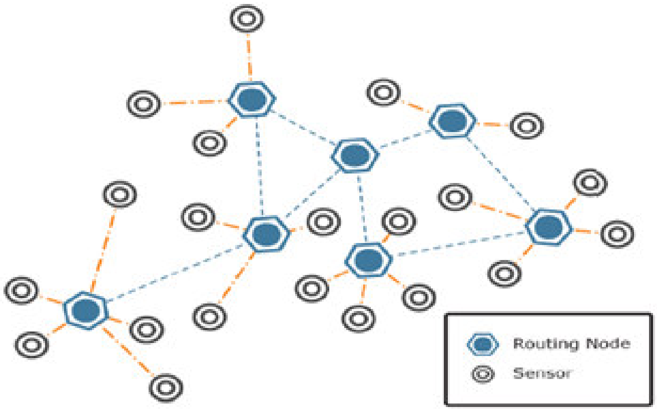

Fig 1: Representative Wireless Sensor Network [4]

2. LITERATURE REVIEW

For the secure network protocol for WSNs, different technologies have been developed, including RM, LSN, SET, Bloom Filter and AICN Protocol [5], Line-Selected Multicast (LSM), and RED protocol [6][8], ECCE, Localized Multicast [7] [11], SPINS[15]. Md. Moniruzzaman, Md. Junaid Arafeen and Saugata Bose et.al present Randomized Multicast (RM), Line Selected Multicast (LSM) protocol used for detection of cloned nodes in wireless sensor network. In LSM as the intermediate nodes check for collusion, it requires less communication than RM protocol. And also cannot predict the location of collusion as all decisions of protocol are made locally and probabilistically. Therefore, LSM shows more fine result against node replication. SET protocol efficiently detects cloned node while it require less message transmission than LSM protocol. This protocol also provides distributed load sharing among the nodes in the wireless sensor network. Another protocol is boom filter. It has ability to detect clone nodes increases with the number of clones.

Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member et.at present RED protocol is similar in principle to the Randomized Multicast protocol. But RED achieves a large improvement over RM protocol in communication and computation terms. When RED compared with LSM, it is more efficient than RM, RED protocol also proves that it is considerably more energy efficient than other. RED is also more robust against attacks. RED executes routinely at fixed intervals of time. Every run of the RED protocol consists of two steps. In the first step, a random value, rand, is shared among all the nodes. This random value can be broadcasted in the network with centralized mechanism.In the second step, each node digitally signs and locally broadcasts its claim—ID and geographic location.. RED protocol is actually independent of the routing protocol used in the network. RED is both ID-oblivious and area-oblivious and also shows a more improvement ii detection capability.

Mauro Conti , Roberto Di Pietro and Luigi V. Mancini et.al presents the ECCE (Enhanced cooperative channel establishment) protocol as a new distributed, probabilistic, cooperative protocol and it used for establish a secure pairwise communication channel between any pair of sensor nodes in a wireless sensor network (WSN). The main use of the ECCE protocol is to allow the set-up of a secure channel between two sensors that do not share any pre-deployed key.

Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar et.al present SPINS which is security protocol for sensor network. SPINS protocol is mainly consist of two secure blocks: SNEP and TESLA. SNEP block provides the number of important baseline security primitives such as Data confidentiality, two-party data authentication, and data freshness. But the difficult problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. Another TESLA is a new protocol which provides authenticated broadcast.

Another security protocols such as Sequential Analysis[12], MiniSec [13], Memory Efficient Protocols[14] in wireless sensor network. J. Ho,M.Wright, and S. K. Das et.al present in their work a replica detection scheme for mobile sensor networks based on the Sequential Probability Ratio Test (SPRT). A protocol SPRT to detect mobile replicas by using the basic idea that a mobile node should never move at speeds in exceed of the system defined maximum speed in wireless sensor network. This protocol quickly detects mobile replicas, Furthermore Secure sensor network link layer protocols such as Tiny Sec ZigBee minisec. However, TinySec required low energy consumption also by reducing the level of security provided by it. In contrast, ZigBee provide high level of security, but this protocol suffers from high energy consumption. Whereas MiniSec is a secure network layer that can be capable of obtaining the best of both low energy consumption and high security. It has mainly two operating modes, one for single-source communicantion.

Ming Zhang Vishal Khanapure Shigang Chen and Xuelian Xiao et.al present another protocol such as memory efficient protocols significantly improves performance by reducing the amount of memory space needed for communication; this is done by balancing the memory and energy consumption across the network. This memory efficient protocol is capable for improving the detection probability to nearly 100%. But this protocol has some limitations such as they cannot detect the replication attacks in a mobile sensor environment

3. OVERVIEW OF PROPOSED METHOD AND CONTRIBUTIONS

Here a secure network protocol for wireless sensor networks is propose which works with Localized Detection, Efficiency and Effectiveness, Network-Wide Revocation Avoidance as well as provide Time Synchronization Avoidance on sensor nodes in the network. This protocol can detect node replication attacks in a localized fashion. This algorithm is a particular type of distributed algorithm. Each node in the localized algorithm can communicate with only its one-hop neighbors in the network. This characteristic is helpful for reducing the communication overhead significantly. Furthermore these algorithms can identify replicas with high detection accuracy. The replica revocation is done by each node without flooding revocation messages in network. Most important feature is time of nodes does not need to be synchronized in the network.

Since the several existing algorithms are built upon several other requirements. But in that algorithms found some common weakness for detecting node replication attacks. Also they required large amount of communication cost is still not controllable.

The rest of the paper is organized as follows: the details for the proposed XED and EDD schemes with corresponding algorithms will be presented in Section V. Afterward, the analytical results, simulation study, and prototype implementation will be presented in Section VI, At last, the conclusion will be made in Section VII

4. SYSTEM MODEL

At first, In this section, we first introduce the network model that is adopted in our method. Then, the security model is described

4.1 Network Model

Assume that the sensor network consists of n sensor nodes with their IDs, {1,…,n} . And this communication of nodes is assumed to be symmetric in the wireless sensor network. In addition to this each node in the network is to be periodically broadcast a beacon to its neighbors which is consisting of its ID. This type of requirement is in various applications, for example, object tracking application. The total time is divided into same length time intervals. Nonetheless, the time between sensor nodes does not need to be synchronized.

None the less, by considering that the replicas do not collude with each other. They can communicate with each other in the network, and also replica can always share the newest received random numbers with the other neighboring replicas, thus degrading the performance of detection because number of replicas is available to reply with the correct random number. Time among sensor nodes does not need to be synchronized.

Each sensor node in the network has mobility and they can move according to the Random Way Point (RWP) model which is commonly used in modeling of sensor networks. Each node is to be aware of its geographic position in the network.

In this model, each node randomly chooses a destination node in the sensing field, and moves toward it with predefined interval. After reaching to the destination node, the node remains static for a random time and then again starts moving according to the same rule. In general, the models used are the same as the ones in prior works.

4.2 Security Model

In our methods, sensor nodes are not tamper-resistant. This means, after sensor nodes are physically compromised only when the corresponding security identity can be accessed. After sensor deployment these sensor nodes could be adjusted by the adversary immediately .The adversary has all of the legitimate identities from the compromised nodes. After having identities of original nodes, adversary deploys two or more nodes with the same ID; i.e., replicas, into the network. After that these replicas can communicate with others and collude with each other in order to avoid replica detection in EDD.

For example, replicas can share their identity with other node in the network and can selectively be silent for a certain amount of time if required after the collusion. By use of the digital signature function, the replicas in the network cannot create a new ID as the nodes being not compromised before, because it is too difficult for the adversary to have the corresponding security identity. Due to this in this paper mainly focus on node replication attack

Since the focus of this paper is on the node replication attack, also many security issues on sensor networks like as key management, replay attack, secure query, etc., we assume that they can be handled very well.

DOI: 10.090592/IJCSC.2016.007

5. PROPOSED METHODOLOGY

In this section, our proposed algorithms, eXtremely Efficient Detection (XED) and Efficient Distributed Detection (EDD), for detection of replica in mobile networks will be described in details as follows:

A. XED

1) Algorithmic Description of XED:

The need of development of XED algorithm is motivated by the observation that, if a sensor node u meets another sensor node v at an earlier time in the network and also sends a random number u to v at that time. And when these u and v node meet again to each other, u can ascertain whether this is v node which met before by requesting the random number to it. In XED algorithm, we assume that the replicas cannot collude with each other in the network but this assumption will be removed in the next solution. In addition to this, all of the exchanged messages between the nodes in the network should be signed unless specifically noted. The XED scheme is mainly consisted of two steps such as offline step and an online step. The offline step is executed before sensor node deployment in the network while online step is executed by each node in the network after deployment.

Offline Step. In offline step of XED, communication between numbers of nodes can be done in the network. For communication purpose initially each node is consist of security parameter p and a cryptographic hash function h(.). And also there are two arrays are used such as $L_r^{(u)}$ and $L_s^{(u)}$ having length of n which is used to keep the received random numbers and the materials used to check the proper received random numbers in order, along with a set $B^{(u)}$ which is use to stored blacklisted nodes that found in the network. Arrays $L_r^{(u)}$ and $L_s^{(u)}$ are initially set to the zero-vectors. Also $B^{(u)}$ is initialized with empty.
Online Step: In online step of XED, while communication between nodes u and v at that time If u encounters v for the first time then u randomly generates the random number α € [1. 2^b - 1] , then compute hash value h(α) , sends this hash value h(α) to v , and stores this value in to $L_s^{(u)}[v]$ = α . Incase if u that knows that it encounters v for the first time if $L_s^{(u)}[v]$ = 0. When u encounters v then before communication it first checks if v is in the blacklist$B^{(u)}$. If so, then this means that is v considered a replica by u and u refuses to communicate with node v. Furthermore blacklist $B^{(u)}$ is to be different for different nodes in the network. This is because each node in the network detects the replica by itself and it will detect the replica at different time. Nonetheless, it is also guarantee that each replica will be blacklisted by all nodes. The effectiveness of XED algorithm is fully depends on the assumption that the replicas do not collude with each other in the network. At the time of communication in the network replica always send newest random number to neighboring replicas. So that it is difficult to detect replica because they reply with correct random number. The solution of this drawback of XED algorithm will be provided in EDD algorithm.

Algorithm: XED-online step

```
// this algorithm is performed by node u at each time t
// $v_1$,…,$v_d$ are the neighbours of u
// {$v_1$,…, $v_d$} € $B^{(u)}$

Set T = 1 and $R^{(u)}$ = φ, u € [1, n]
Set $L^u[i]$ = 0, 1 ≤ i≤ n, u €[1, n]
Repeat
    T = T+ 1,
  Calculate µ1, µ2, $\sigma_1^2$ and $\sigma_2^2$
  Set $Y_1$ = µ1 + 3$\sigma_1$ and $Y_2$ = µ2 - 3$\sigma_2$
Until $Y_1$ □ $Y_2$
Set □ = $\frac{Y_1-Y_2}{2}$
```

B. EDD

1) Algorithmic Description of EDD: In EDD algorithm the communication between node u and v. The maximum number of times Y1 that node u encounters node v and this should be limited with high probability in fixed period of time in the network. While on the other hand the minimum number of times Y2 that node u encounters the replicas with the same ID v in the

DOI: 10.090592/IJCSC.2016.007

network should be larger than a threshold in the same period of time. So that it has the ability to identify the replicas. Also that it overcome drawback of XED that replicas can collude with each other in EDD.

In addition to this, unless specifically noted all the exchanged messages between nodes should be signed. Mainly EDD algorithm is consist of two steps such as an offline step and an online step. The offline step is performed before sensor node deployment. Before communication calculate the parameters such as length T of the time interval and the threshold used for discrimination between the genuine nodes and the replicas. On the other side in the online step will be executed by each node after each move. Then each node checks whether the encountered nodes are replicas or not by comparing □ with the number of encounters.

Offline Step. The offline step of EDD in which is consist of array $L^{(u)}$of length n-1 is used to store the number of counters of each node in a given time interval. And set $B^{(u)}$ contains the IDs that have been considered u as replicas.

Algorithm: EDD_offline step

```
Set T = 1 and $B^{(u)}$ = φ, u € [1, n]
Set $L^{u}[i]$ = 0, 1 ≤ i≤ n, u €[1, n]
Repeat
      T = T+ 1,
  Calculate μ1, μ2, $\sigma_1^2$ and $\sigma_2^2$
   Set $Y_1$ = μ1 + 3$\sigma_1$ and $Y_2$ = μ2 - 3$\sigma_2$
Until $Y_1$ □ $Y_2$
Set □ = $\frac{Y_1 - Y_2}{2}$
```

Online Step: In online step of the EDD algorithm in which the beginning of each time interval each node has a counter to record the elapsed time.

After time units t is completed means t>T then the counter t is reset. The beginning of a new time interval is simply represented by " t= t_0" When each time a node finds another node then the corresponding value in the list $L^{(u)}$ [v] is increased by 1. If the value of u node $L^{(u)}$ [v] is larger than the threshold □ then node u is blacklisted by node v. This is because number of encounter of node is greater than □.

In additional to this the storage overhead is O(n), which is not scalable in case of the network size. Due to this a sketch-based technique is used to reduce the storage overhead.

Finally the effectiveness of EDD is fully depends upon each node is not only faithful but also periodically broadcasts its ID in the network. And this method is called *selective silence* which could be taken by the replicas to lower the detection capability of EDD.

Algorithm: EDD_online step

```
// this algorithm is performed by node u at each time t
// $v_1$,…,$v_d$ are the neighbours of u
// {$v_1$,…, $v_d$} € $B^{(u)}$
Broadcast beacon $b_u$ //$b_u = \{u\}$ contains the ID of u
If t ≠ $t_0$
        Receive beacon $b_{v1}$,…, $b_{vd}$
        For k = 1 to d
             $L^{(u)}[v_k]$ = $L^{(u)}[v_k]$ + 1
              If  $L^{(u)}[v_k]$ □ □ then set $B^{(u)}$ = $B^{(u)}$ U {$v_k$}
Else //t = $t_0$
     Set $L^{(u)}[s_k] = 0$, k = 1,…,n
```

6. EXPERIMENTAL RESULTS AND ANALYSIS

6.1. Simulation Setup For our experiments, we simulate an environment with graphical representation of 100 different sensor nodes randomly Placed at different locations in the field of size (700m × 800m). The performance analysis of system is made on Windows based platform under Java Universal Grange Framework (JUNG) [16]. Java software development kit with minimum 1.5 versions or higher and eclipse/net beans IDE is used for simulating the system. Nodes are simulated using the Graphical representation in Java through AWT and swing based classes and using event handling.

Table 1: Simulation Parameter

Parameters	Value
Simulation Model	Default Random Waypoint
Simulation Area	700 metersX800meters
MAC	IEEE 802.11
No of Nodes	1 to 100
Communication range	1 to 250 meters
Energy	Max Up to 200 J
Packet Length	1024 bytes
Distance between Sensor Nodes	Pixel Range
Simulation Time	200 seconds

6.2 Analysis Result

Different many types of experiments have been done to evaluate the performance and accuracy of the enhanced Security protocol for WSN using the different security scheme. In this case, our analysis focus on two localized algorithms for detection of node replication attack, on the basis of the memory overhead, detection accuracy, detection time, energy consumption. Here we compare the XED and EDD algorithm and results of these is summarized in table 2.

The effectiveness of XED algorithm is fully depends on the assumption that the replicas do not collude with each other in the network, which obviously holds. Nevertheless, the performance of EDD varies according to different network settings. Thus, In this section validating the effectiveness of EDD algorithm through a simulation. Here we discuss how the parameters, such as detection accuracy, detection speed and energy consumption affect in the detection.

Table 2: Analysis Result

Factors	XED	EDD
Detection Accuracy	Almost perfect	Perfect
Storage Overhead	Value of U, V	Counter list, Black list
Computation Overhead	Random nu Hash Value Verification of hash	Calculation of Threshold
Communication Overhead	Exchange 2 values first time Exchange two values second meet	No communication

Table 2 reports the results of the implementation of the proposed XED and EDD algorithms. Here memory consumption that the program size reported i.e. RAM and ROM in Bytes. This program code for not only used for checking mechanism of proposed methods but also use for many communication mechanisms that are commonly required by many other sensor network applications. Thus, the program size reported could be an overestimation. Next parameter is detection time of proposed

DOI: 10.090592/IJCSC.2016.007

methods. Since the detection time incurred by the calculation is less than one second in XED and is even less than 0.1 seconds in EDD. Last parameter, energy consumption needed for the execution of XED and EDD algorithms which is different for different cases like CPU, radio and overall.

6.2.1 Detection Time and Detection Accuracy

As shown in below Figures, it can be easily noticed that when the number of movements increases in an interval, it becomes easier to differentiate between the network node and replicas. Here, "easier" means detection accuracy is higher. This is because as number of movement increases in each interval then it becomes very closer to replicas. Although increasing the time interval size can be useful for the detection accuracy, however, bur the improvement of detection accuracy cannot be unlimited.

Our experience shows at least the detection accuracy of both XED and EDD algorithms is achievable even if there are number of nodes are increases to detect replicas in the network.

6.2.2 Energy Consumption

In figure 4, where the energy consumption can be shown. The time we conducted the simulation was 200 seconds. Similar in memory consumption in which the energy consumption can be an overestimation because the energy consumption incurred by data transmission. The main goal of energy consumption is to reduce the amount of energy required to provide services. There are different many motivations to improve energy efficiency. Reducing in energy use reduces energy costs and this may result in a financial cost also saving. So energy efficiency has prove to be a cost-effective for building economies without necessarily increasing energy consumption. As shown in below figure 4 the energy consumption of XED and EDD algorithms in XED consume more energy than EDD.

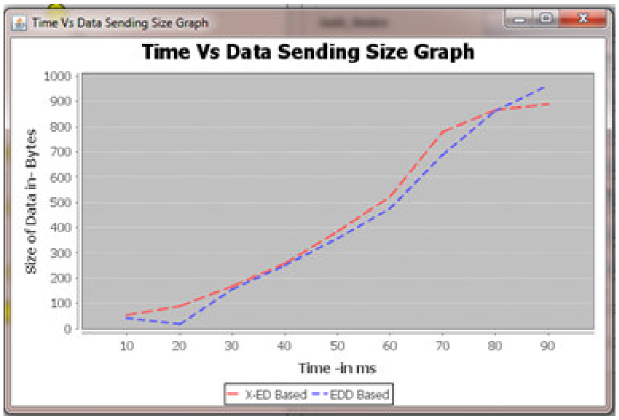

Figure 2: Detection Time

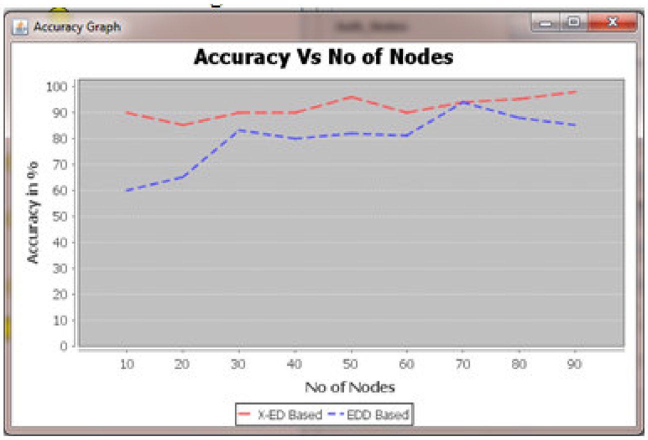

Figure 3: Detection Accuracy

DOI: 10.090592/IJCSC.2016.007

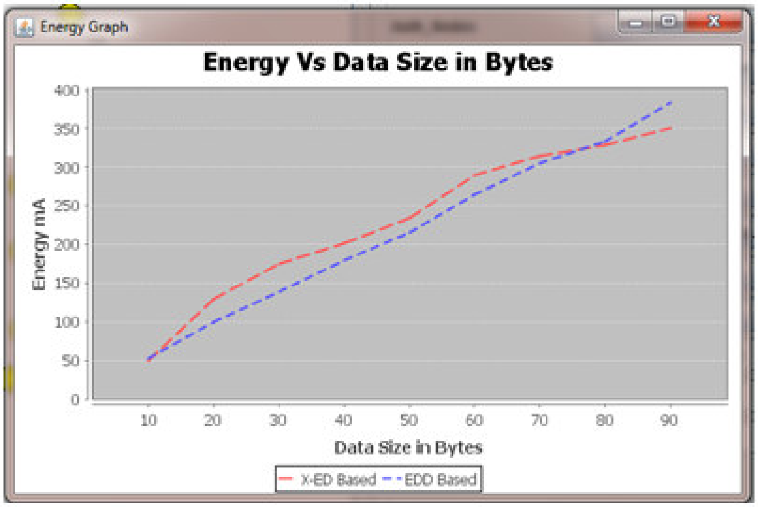

Figure 4: Energy Consumption

7. CONCLUSION

In this paper, the method proposed is implemented on Windows Java Universal Graph Framework. It is an efficient network layer security system and is the fully implemented security mechanism, i.e. two replica detection algorithms such as XED and EDD for wireless sensor network. Although the effectiveness of XED algorithm is fully depends on the assumption that the replicas do not collude with each other in the network in its detection framework. Notably, the drawback of XED algorithm is overcome in EDD algorithm which is fundamentally different from those used in the existing algorithms. EDD is not achieves good balance among storage, computation, and communication overheads and also include unique characteristic like network-wide time synchronization avoidance and network-wide revocation avoidance in the detection of node replication attacks in WSN.

REFERENCES

[1] Wei Hong David E. Culler, "Wireless Sensor Networks: Introduction," *Communications Of The ACM*, vol. 47, no. 6, pp. 30-33, June 2004.

[2] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, “Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks” *Proc.IEEE transactions on information forensics and security,* vol. 8, no. 5, may 2013

[3] Raju M, Selvan M, “An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey,” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 192-196, 2014.

[4] Mrs: Suvarna Game, Mr. Chandrashekhar Raut, “Protocols for detection of node replication attack on wireless sensor network,” *IOSR Journal of Computer Engineering (IOSR-JCE*), Volume 16, Issue 1, PP 01-1, Jan. 2014.

[5] Md. Moniruzzaman, Md. Junaid Arafeen, Saugata Bose, “Overview of Wireless Sensor Networks: Detection of Cloned Node Using RM, LSN, SET, Bloom Filter and AICN Protocol and Comparing Their Performances,” *International Journal of Digital Content Technology and its Applications,* Volume 3, Number 3, September 2009

[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, “Distributed detection of clone attacks in wireless sensor networks,” *IEEE transactions on dependable and secure computing* ,vol. 8, no. 5, pp. 685–698, Sep./Oct. 2012.

[7] Mauro Conti *, Roberto Di Pietro, Luigi V. Mancini, “ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks’” *Ad Hoc Networks 5*, pp. 49–62, 2007.

[8] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,” in *Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, Montreal, Canada, pp. 80–89, 2007.

[9] Pooja Chaturvedi, Shyam S. Gupta, “Detection of Node Replication Attacks in Mobile Sensor Networks Using Localized Algorithms,” *(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 5 (6), pp.7922-7926, 2014.

[10] S.Dhanalakshmi, S.Kaliraj, Dr.J.Vellingiri, “Efficient and Effective Detection of Node Replication Attacks in Mobile Sensor Networks,” *International Journal of Engineering Research and Development, Volume 8, Issue 10, PP. 26-31, October 2013.*

DOI: 10.090592/IJCSC.2016.007

[11] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks*," IEEE transactions on mobile computing*., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[12] J. Ho, M.Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM)*, Brazil, pp. 1773–1781, 2009.

[13] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in *Proc. Int. Conf. Information Processing in Sensor Networks (IPSN)*, Cambridge, MA, USA, 2007.

[14]M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in *Proc. IEEE Int. Conf. Network Protocols (ICNP)*, Princeton, NJ, USA, pp. 284–293, 2009.

[15] R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar A. Perrig, "SPINS: security protocols for sensor networks," in *International Conference on Mobile Computing and Networking,* pp. 189–199, 2001.

[16] Joshua Madadhain, Danyel Fisher, "Analysis and Visualization of Network Data using JUNG". [Online].http://www.jstatsoft.org/