Detection of Replica Node Attack Based on Hybrid Artificial Immune System Technique

[1]Ms. L. S. Sindhuja, [2]Dr. G. Padmavathi

[1]Research Scholar, [2]Professor and Head,
Department of Computer Science, Avinashilingam University, Coimbatore

Abstract- In the recent years, Wireless Sensor Networks (WSNs) provide an economically feasible solution to a diversity of applications. The applications include object tracking and environmental monitoring. However, security of sensor nodes is critical because of the unattended nature of the network and thus they are prone to many attacks. One such attack is the node replication attack which corrupts the entire network by compromising few sensor nodes. Few of the techniques are proposed to detect the node replication attack using witness finding strategy and centralized detection methods are used for static networks. These methods incur high communication and memory overheads and induce problems related to security and efficiency. This paper proposes to solve these issues using Enhanced eXtremely Efficient Detection (Enhanced XED) and integrated Artificial Immune Systems (iAIS) model to detect the clones which are not resilient against collusive replicas. The advantages of the proposed method include (i) increase in the detection rate, (ii) decrease in the false rates, (iii) effectiveness and (iv) low energy consumption. The performance of the proposed work is measured using Bandwidth, Message drop, Energy, Overhead, Average Delay and Packet Delivery Ratio. The implementation is done using ns2 to exhibit the actuality of the proposed method.

Keywords- Wireless Sensor Networks, Node replication attack, B- cells, Dendritic Cells, eXtremely Efficient Detection

1. Introduction

A Wireless Sensor Network (WSN) comprises of a number of resource constrained sensor nodes. WSNs are generally deployed in harsh and hostile environment. The applications of WSN range from object tracking to environmental monitoring. Security of WSN is a crucial task. WSNs are often unattended and are prone to different kinds of attacks which includes jamming and eavesdropping in the network. Out of these attacks node replication attack is a vulnerable one as it may cause injection of false data in the network or it may even cause a wormhole attack. The node attack compromises a sensor node and replicates it by gathering the secret information and deploys in the network.

A collection of methods have been proposed to detect replica nodes in static [2-4] and also in mobile WSNs [5-8]. In the static WSNs, the detection methods detect the cloned nodes in a distributed approach rather than the centralized one. In the distributed approach, a set of witness nodes are used for detection process. In which it employs the information that nodes which have the same ID at different locations are detected as replicated nodes.

The detection methods in mobile WSNs are generally classified as centralized method, hypothesis method and distributed encounter methods. Based on the hypothesis testing, a node broadcasts its location ID when it enters a communication range. The base station receives the location of the new node probabilistically from the set of nodes in the communication range. The base station, then evaluates the velocity of the newly arrived node and analyze it to the limits defined by the system. A subsequent number of samples about a particular node are collected by the base station to decide whether it is a cloned node or not. In the encounter based methods, a random number is exchanged when two nodes meet for the first time. When they happen to meet again, they examine each other for the exchanged numbers. When a particular node fails to respond with the correct random number they are detected as a replicated node.

The node replication attack induces some negative effects in the network. The undetected malicious clones affect the operations of the network. The detection methods introduce an added storage and communication overheads in the network. At last, few detection methods incorrectly recognize, a subset of valid nodes as replicated nodes and revokes the detection process. As a consequence, these nodes are inadequate to perform the operations of the communication and sensing protocols of the network thereby the performance of the WSN is degraded.

The main objective of this work is to accurately detect the self/non self-nodes from the sensor network. This is considered as a necessary process because the node replication attack is significantly harmful to the networks because the replicas, which have legitimate keys and are controlled by the adversary, can easily launch the insider attacks without easily being detected. The hybrid technique is done by hybridization of the distributed replica detection scheme, XED with iAIS model. Initially nodes are presented to the XED, where communication cost can be fixed and location information of the node is not required for detection of replication nodes. Then detected replica nodes are passed to the iAIS which further checks the nodes with certain conditions and finally desires the node as replica or not. By this hybrid technique, detection accuracy can be maximized.

This paper constructs as follows, Section 2 describes the previous works done for this application followed by its merits and demerits. Section 3 explains about the proposed work of XED how it solves the optimization problems, and integrated AIS model which detects the replica nodes in detected clones. In Section 4, evaluation results are provided for the proposed work and it is compared with the existing work. The final conclusion of this work is given in Section 5.

2. Literature Survey

Randomized Multicast (RM) is the first protocol proposed by Parno et al [2], which distributes location claims to a randomly selected set of witness nodes. The second protocol, Line-Selected Multicast (LSM), exploits the routing topology of the network to select witnesses for a node location and utilizes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbors. Then, the witness nodes are randomly selected within the communication range by each neighbors to forward the location claim. When there exists a conflicting location claim in one of the witness nodes, then the replicated node exists in the network. The main aim of the LSM is to reduce the communication cost and to increase the detection probability. The intermediate nodes stores the location claim and act as witness nodes. With the help of these intermediate nodes, a line is drawn across the network and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

Kai Xing [9] proposed two replication detection schemes (Time Domain Detection (TDD) and Space Domain Detection (SDD)) to undertake challenges from both the time domain and the space domain. This theoretical analysis indicates that TDD and SDD provide high detection accuracy and excellent resilience against smart and colluding replicas and have no restriction on the number and distribution of replicas. The method also incurs low communication overhead. The TDD and SDD are the only approaches that support mobile networks and place no restrictions on the number and distribution of the cloned frauds and also on whether the replicas collude or not.

Location-aware clone detection protocol successfully detects clone attack proposed by Zhongming et al's [10] which has little negative impact on the network lifetime. Probably, the location information about sensors and randomly select witness nodes are utilized in a ring area to verify the privacy of sensors and to detect cloned attacks. The ring structure facilitates energy efficient data forwarding along the path towards the witnesses and the sink. The traffic load is distributed across the network, which considerably improves the network lifetime. This protocol gives the result of maximum clone detection probability with trustful witnesses.

Conti, M [11] proposed a method to detect the node replication attack. This work is processed in two steps: First, the desirable properties of a distributed mechanism for the detection of replicated IDs is analyzed; second, a distributed solution is proposed for the detection of replicas that does not completely fulfill the requirements. Thus, the design of efficient and distributed protocols to detect node identity replicas is still an open and demanding issue.

Ho et al. [3] introduced a detection scheme for mobile sensor networks, which follows sequential probability ratio test. However, the efficiency of this scheme relies on the involvement of the base station, easily incurring the problems of single-point failure and fast energy depletion of the sensor nodes around the base station.

A novel protocol, called eXtremely Efficient Detection (XED), is proposed by Chia-Mu Yu et al [6], to resist against node replication attacks in mobile sensor networks. The merits of XED include (i) only constant communication cost is required for replica detection; (ii) sensor nodes location information is not required. Performance analyses and comparison with other methods demonstrate the effectiveness of this protocol. A comparison of the existing detection methods is done and Table 1 summarizes the same.

Table 1 Survey on various techniques

Year	Author	Techniques	Observations
2005	B. Parno, A. Perrig, and V. Gligor	Randomized Multicast and Line-Selected Multicast	Reduce the communication costs Increases the probability of detection
2008	Ho et al	Sequential Probability Ratio	Easily incurring the problems of single point failure Fast energy depletion of the sensor nodes around the base station
2008	Chia-Mu Yu et al	Extremely Efficient Detection (XED)	Constant communication cost is required Sensor nodes local information is not needed
2010	Kai Xing	Time Domain and Space Domain Detection	Resilience against smart attacks No restriction on number and distribution of the replicas
2013	Zhongming et al	Location-aware clone detection protocol and Ring area to verify the privacy of sensors	Produces maximum clone detection probability with trustful witnesses

Due to the literature survey, it is observed that XED algorithm is efficient in terms of communication cost. Hence an attempt has been made to improve the existing XED algorithm in terms of detection accuracy. The next section discusses the proposed method.

3. Proposed Method

The proposed work [1] [12] here is done by using XED analysis and it is combined with the concepts of B-cells, T-cells and Dendritic Cells in a unified system. In this section, XED is analyzed which is widely used for detection of clones in mobile WSNs.

The XED method is one of the information exchanged based detection method. In which the detection is based on the information exchanged and not based on the location information. In the XED method, the detection is based on the challenge and response strategy. The challenge and response strategy describes that if the nodes s1 meets another node s2 for the very beginning time, then random number is generated and it is added to the random number set. After that, when it meets further, request is generated for issuing random number and it is checked with the random number which is already generated.

When the generated random number does not match, then they are marked as replica node and added to the replica node set. Meanwhile, if it matches, it is marked as self, node and added to that set. The XED method is effective only when there is no communication between the replicas. When the communication happens to occur, then they can exchange the recently shared random number. As a result, the detection ability is degraded. In order to overcome the above drawback, the Enhanced XED method is proposed using the packet loss (PL) and average efficiency, which are calculated for each and every node in the network. When the PL occurs, they are taken upon for further processing, but if does not occur, then the node is sent to the self-node set.

When the PL has occurred, the average efficiency of the nodes is calculated. After that a threshold is assigned and if the node has a greater threshold value, then the average efficiency of each node is compared with the existing random number set. If the matching between them occurs them occurs immediately they are stored in the self-node set and marked as semi- mature DC. Otherwise the node is compared with the replica node set. If it matches, then they are stored in the replica node set and mark them as mature DC.

The confession of replica detection is done using enhanced XED alone. The proposed method employs integrated Artificial Immune System (iAIS) for further decision process. The obtained mature DC and the semi mature DC sets are passed to the iAIS.

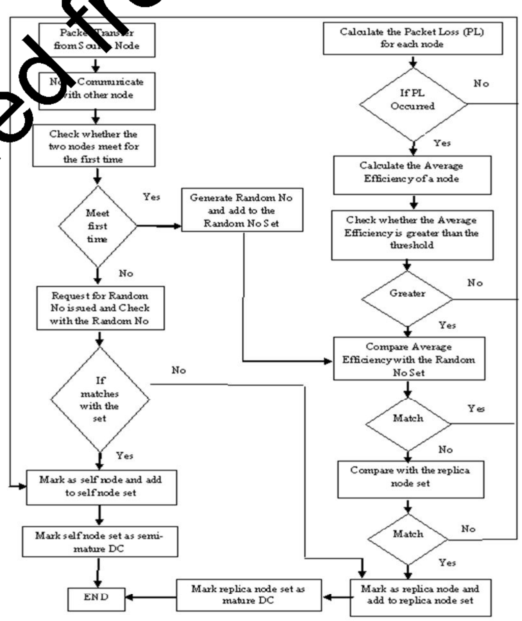

Figure 1: Flow Diagram of Enhanced XED

 ISBN : 978-81-925233-5-4

A. Detection using an Integrated AIS Model (iAIS)

In the literature for obtaining secure routing in MANETs neither self/non-self nor danger theory paradigm is used. Here the combining concepts of B-cells, T-cells and Dendritic Cells (DCs) in a unified system are used with an enhanced XED method for clone detection.

The B- cell model does the activity of adaptive immunity, which removes the antigens by launching an attack. It is presented by using the classical context of the self-non- self-discrimination paradigm. The two phases of the B- cell model are the learning phase and the operational phase. The benign behavior of the system is done in the learning phase. Whereas, in the operational phase, the received antigen is classified as self or nonself.

The basic model of the DCs is inspired from the innate immune system. The innate immune system is an in built immune system that defends against the antigens. The DCs act as a first line of defense. It represents the functional behavior starting from sampling Ag in the tissue till determining the context of the tissue as safe or dangerous. The DCs determine the co- stimulation level by processing the signals which are present in the tissue at the time of sampling. When the co- stimulation threshold exceeds, then the dangerous context is transformed to the mature state and the safe context is transmitted to the semi- mature state.

To present the sampled Ags by DCs in thymus and maturation/activation of T-cells the basic Dendritic cell model is extended. Here the result of the enhanced XED model, namely the two states mature and semi-mature states are migrated to the thymus and check the sampled Ags from the enhanced XED method to the T- cells.

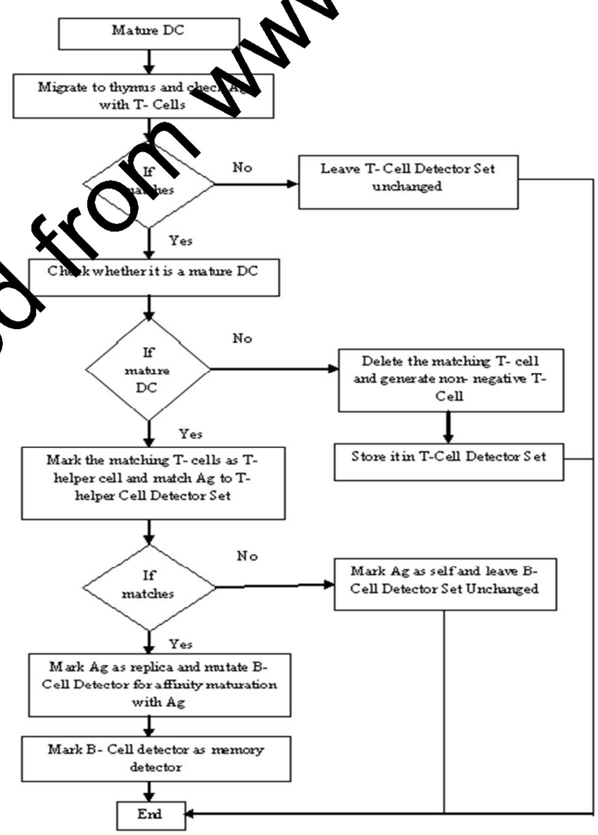

Figure 2: Flow Diagram of iAIS

 ISBN : 978-81-925233-5-4

When the matching occurs between the sampled Ags and the T- cells, again, it is checked whether it is a mature DC. If it is a mature DC, then the appropriate T- cells are marked as T- helper cell and stored it in the T- helper cell detector set. The incoming Ags is matched with the T- helper cell detector set. If it matches, then the Ag is declared as non- self. The B- cells are mutated for affinity maturation. The detected B-cells are marked as memory detector. Otherwise the B- cell detector set is marked as unchanged and they are declared as self-node. The pseudo code of the proposed methodology is illustrated in Table 3

Table 3 Pseudo code for proposed methodology

```
Input: packet
Declare: Average efficiency as AE and packet loss as PL
Output:  replica node  or self node
Algorithm
        For each packet transfer from source node
        While not destination node do
                Node communicate with other node
                If (meet first time) then
                    Generate random number and add to random number set
                Else
                    Request for random number issued
                If (random number issued is match random number set) then
                    Declare as self node
                Else
                    Declare as replica node and add replica node to replica set
                End if
                End if
                Calculate PL for each relay nodes
                If (PL is occurred) then
                   Calculate AE of a node
                If (AE > threshold) then
                  Compare the AE with random number set
                If (match) then
                  Declare as self node
                Else
                   If (node is matched with the replica node set) then
                   Declare as replica node
                End if
                End if
                 Migrate Replica node to thymus
                 Check Ag with T cells
                If (match) then
                If (Mature DC) then
                  Matching T-cell become T-helper Cell
                  Add to T-helper cell detectors Set
                  Match Ag to T-helper cell detector
                If(match)then
                   Declare Ag as non self Ag
                   Mutate B- cells detector for affinity maturation with Ag
                   Mark B-cells detector as memory detector
                Else
```

```
                    Declare Ag as self Ag
                    Leave B-cells detector Set unchanged
                 End if
                 Else
                    Delete matching T- cell
                    Generate non-negative T-cell
                    Add to T-cells detector Set
                 End if
                 Else
                     Leave T-cells detector DB unchanged
                 End if
                 End if
                 Else
                     Declare as self node
         End if
         End if
         Else
            Declare as self node
         End if
         End while
         Next
```

4. Experimental Analysis

In the experimental analysis, the mobile based sensor network behavior and its performance are analyzed with proposed Hybrid Enhanced XED – iAIS method. The analysis is made in the hybrid techniques Enhanced XED combined with integrated AIS model. The simulation parameters used while implementing this technique is summarized below in the Table 4.

Table 4 Simulation Parameters

Simulation Parameter	Value
Propagation	TwoRayGround
Mac	802_11
X dimension of the topography	1000
Y dimension of the topography	1000
Adhoc Routing	AODV
No of nodes simulated	50
Cp	Cbr10
Sc	nodes50mob
Simulation time	500 seconds
Energy	EnergyModel
Initial Energy	1000000
Bcell_detectorRef	5
Bcell_detectorThr	4
Aodv Minimum Neighbor	6
Aodv Security Duration	2

The performance of this work is measured using the bandwidth, message drops, energy, overhead, average delay, PDR graphs which shows its efficient result towards the clone detection and identification of replica nodes in WSN. These results are discussed briefly below

The values obtained for routing packets, packet delivery ratio, normalized routing load, routing overheads, average Hop Counts, Average Delay in seconds, dropped data packets and dropped data bytes shows this efficiency towards clone detection in WSN.

Bandwidth - The bandwidth is defined as the maximum amount of data that can be transferred between the two nodes without disturbing the other progress in the network.

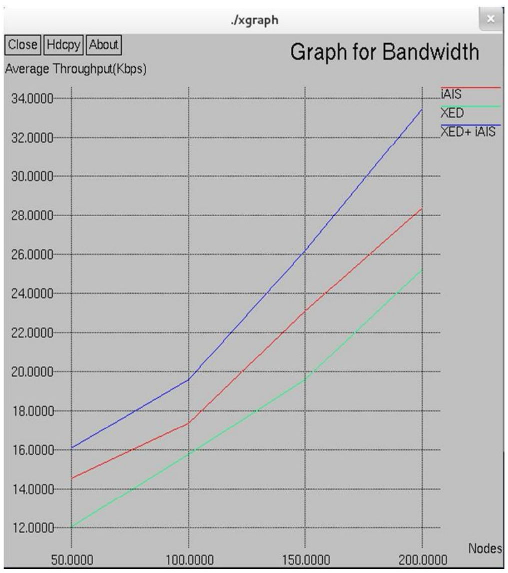

Figure 3: Comparison Graph for Bandwidth

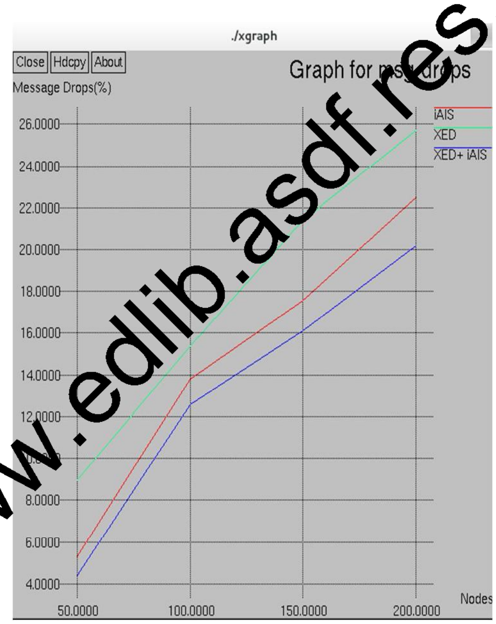

Figure 4: Comparison Graph for Message-Drop

The Figure 3 shows the bandwidth graph for AIS, XED and for Hybrid Enhanced XED-IAIS. Where, XED shows higher bandwidth value and proposed Hybrid Enhanced XED-IAIS takes lesser bandwidth than the both. And here the node formation in mobile WSN is shown behind it.

Message Drops - This metric represents the overall system loss when it is in an unsustainable state.

The Figure 3 shows the graph of message drops for AIS, XED and for Hybrid Enhanced XED-iAIS. Where, XED shows higher message drops value and proposed Hybrid Enhanced XED-IAIS takes lesser message drops than the both.

Energy - The percent energy consumed by a node is calculated as the energy consumed to the initial energy. And from that finally the percent energy consumed by all the nodes in a scenario is calculated as the average of their individual energy consumption of the nodes as defined in equation (1).

$$Average\ Energy\ Consumed = \frac{Sum\ of\ Percent\ Energy\ Consumed\ by\ all\ nodes}{Number\ of\ Nodes} \qquad (1)$$

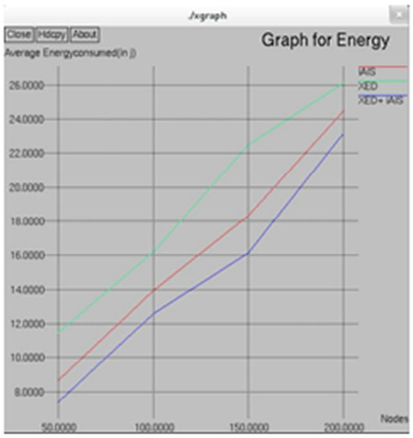

Figure 5: Comparison Graph for Energy

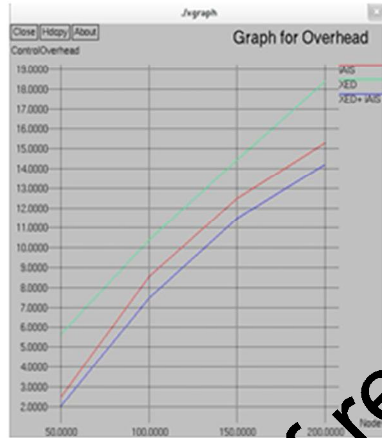

Figure 6: Comparison Graph for Overhead

The Figure 4 shows the graph of energy required for AIS, XED and for Hybrid Enhanced XED- iAIS. Where, XED takes higher energy and proposed Hybrid Enhanced XED- iAIS takes lesser energy than the others.

Overhead - This is the ratio of total numbers of control packets generated to the total number of data packets received during the simulation time given in equation (2).

$$overhead = \frac{data\ packets\ received}{control\ packets\ generated} \qquad (2)$$

The exceeding Figure 5 shows the graph of overhead for AIS, XED and for Hybrid Enhanced XED- iAIS. Where, XED takes higher overhead and proposed Hybrid Enhanced XED- iAIS takes lesser overhead than the others.

Packet Delivery Ratio (PDR) - The ratio between the numbers of packets successfully received at the destinations and the total number of packets sent by the sources defined in equation (3).

$$PDR = \frac{received\ packets}{sent\ packets} * 100 \qquad (3)$$

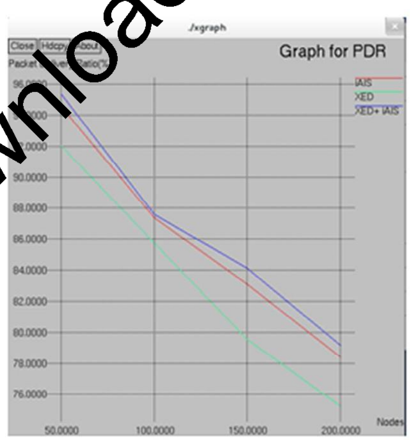

Figure 7: Comparison Graph for PDR

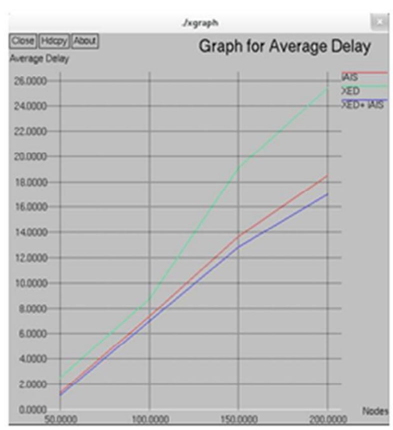

Figure 8: Comparison Graph for Average Delay

The Figure 6 shows the graph of PDR for AIS, XED and for Hybrid Enhanced XED- iAIS. Where, XED takes higher PDR and proposed Hybrid Enhanced XED- iAIS takes higher PDR while comparing with each other.

Average Delay - The average delay is calculated by taking the average of delays for every data packet transmitted to the total number of received packets as defined below in equation (4). The parameter is measured only when the data transmission has been successful.

$$Average\ Delay = \frac{Sum\ of\ All\ Packets\ Delay}{Total\ No\ of\ Received\ Packets} \quad (4)$$

The exceeding Figure 7 shows the graph of average delay taken for AIS, XED and for Hybrid Enhanced XED- iAIS. Where, XED takes more average delay and proposed Hybrid Enhanced XED- iAIS takes less average delay while comparing.

The overall comparison results for the bandwidth, Message drop, Energy, Overhead, Average delay and the PDR is shown in the table below.

Table 5 Results comparisons of proposed hybrid enhanced XED - iAIS with XED

Metrics	Existing Techniques Result (Kbps)	Proposed Techniques Result (Kbps)	Improvement (%)
Bandwidth	28,0000	3[illegible],0000	17.8
Message drop	22,0000	20,0000	9
Energy	24,0000	23,0000	4.1
Overhead	15,0000	14,0000	6.6
Average	18,0000	17,0000	5.5
PDR	78,2000	79,0000	1.0

The above Table 5 clearly shows the percentage of improvement achieved for various performance metrics of the proposed technique Hybrid Enhanced XED- iAIS method while compared with existing XED. The proposed work improves its performance in all the metrics, where the bandwidth is improved much better than other metrics.

5. Conclusion

In mobile WSN, clone detection is a present issue where they are affected by a node replication attack. The proposed work studied replica detection methods used to mitigate node replication attack. The proposed work is extended by combining integrated Artificial Immune System, which is energy efficient, reducing processing overheads and it is suitable for deployment on identifying replica nodes in mobile WSN. The experimental analysis graphs of proposed Hybrid Enhanced XED- iAIS are compared with existing AIS and XED which shows that average delay, energy, overhead and message drops of Hybrid Enhanced XED- iAIS is minimum with higher PDR value. This proves that the proposed technique of XED with integrated AIS is efficient towards clone detection and replica identification.

References

1. Tamara Bonaci, Phillip Lee, Linda Bushnell, Radha Poovendran, “A convex optimization approach for clone detection in wireless sensor networks,” Elsevier, Pervasive and Mobile Computing, Vol 9, 2013, pp. 528–545.
2. Parno, A. Perrig, and V. D. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symposium on Security and Privacy, 2005, pp. 49–63.

3. M. Conti, R. Di Pietro, L. Mancini, A. Mei," A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks", in Proc . 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2007, pp. 80–89.
4. Zhu, V. Addada, S. Setia, S. Jajodia, S. Roy, "Efficient distributed detection of node replication attacks in sensor networks", in Proc. 12th Asia- Pacific Conference on Advances in Computer Systems Architecture, 2007, pp. 257- 267.
5. J. Ho, M. Wright, S. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis", in Proc. 28th IEEE Conference on Computer Communications, 2009, pp. 1773–1781.
6. Yu, C. Lu, S. Kuo, "Mobile sensor network resilient against node replication attacks", in Proc. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2008, pp. 597–599.
7. C. Yu, C. Lu, S. Kuo," Efficient and distributed detection of node replication attacks in mobile sensor networks", in Proc. 70th IEEE Vehicular Technology Conference Fall, 2009, pp. 1–5.
8. X. Deng, Y. Xiong, D. Chen, "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks", in Proc. 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2010, pp. 225–232.
9. Kai Xing; Xiuzhen Cheng, "From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad Hoc Networks," INFOCOM, 2010 Proceedings IEEE , 2010, pp.1-9.
10. Zhongming Zheng; Anfeng Liu; Cai, L.X.; ZhiGang Chen; Xuemin Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in INFOCOM, 2013 Proc. IEEE , 2013, pp.2436-2444.
11. J. Ho, M. Wright, and S. K. Das," Fast Detection of Node Replication Attacks in Mobile Sensor Networks," in Proc. IEEE International Conference on Network Protocols, 2008.
12. N. Mazhar, M. Farooq," A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols", Elsevier, Applied Soft Computing, Vol.11,2011, pp. 5695- 5714.