International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 185-202
http://dx.doi.org/10.14257/ijsia.2015.9.4.18

Clone Detection Using Enhanced EDD (EEDD) with Danger Theory in Mobile Wireless Sensor Network

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

[1]Research Scholar, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore
[2]Professor and Head, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore
sindhujakarthick2011@gmail.com; ganapathi.padmavathi@gmail.com

Abstract

In the recent years, Wireless Sensor Networks (WSN) are widely used to reap the benefits of sensing capacity of mobile nodes and its wireless mode of communication. Sensor network architectures can be used for various applications that include intrusion detection, military patrols, border monitoring, etc. The security of nodes in a sensor network is a challenging issue as they are easy targets for attacks. The node replication attack is one among those attacks. The adversary can capture security credentials from a node by compromising the node. The adversary can replicate the node using the same ID. To rectify this problem in a sensor network, various replica node detection techniques have been proposed. These techniques do not work well when multiple replicas are introduced in the network against genuine nodes. Subsequently, the detection capability of the network is degraded. To overcome these problems, this paper proposes Enhanced Efficient Distributed Detection (EEDD) algorithm. It combines the best features of EDD and danger theory of artificial immune system. This hybrid approach EEDD detects the clones. This method prevents multiple replicas in the WSN. The advantages of the proposed method include (i) increased detection rate, (ii) decreased overheads, (iii) high Packet Delivery Ratio (PDR) and (iv) low energy consumption. The proposed method is tested in a simulated environment.

Keywords: *intrusion detection, sensing capacity, node detection techniques, Enhanced Efficient Distributed Detection, detection rate, decreased overheads.*

1. Introduction

Compared to adhoc networks, sensor networks have the distinguishing features like higher number of nodes and their dense deployment to ensure coverage and connectivity. Tens to thousands of nodes in WSNs share the sensed and processed information by communication through wireless channels. The tiny sensor nodes participating in the communication have sensing and data processing capabilities [1]. Due to this, WSNs are vulnerable to a variety of attacks during communication [2].

The replica node attack is a hazardous attack wherein an adversary proceeds with the secret key and ID captured from a compromised node and replicates them in the network [4]. In order to communicate on the network, these replicas make use of the software and the keying materials captured from the compromised nodes. The adversary that controls the replica nodes behave like an authorized node in the network using the captured keying material. To ensure security of sensor networks, communication protocols would allow replica nodes to create pairwise shared keys with other nodes and the base station,

ISSN: 1738-9976 IJSIA

thereby, enable the replica nodes to encrypt, decrypt, and authenticate all of their communications as if they are also genuine nodes [5].

Different node replication attack detection methods proposed in the literature [5, 6, 7, 8, 9, and 11] can effectively detect the attacks only under stable conditions. However, the sensor nodes in many applications have to communicate over an unreliable and unstable medium. Based on the application requirements, they have to communicate using constrained resources with scalability. The existing centralized mechanisms not only fail in an unstable environment, but also not suitable for applications with constrained resources.

In static networks, the problem of node replication detection has been analyzed in various schemes. Only few schemes are available in mobile sensor networks [5, 6, 7, 8, 9, and 11]. Due to mobility, the difficulty arises in the detection of replicas in mobile sensor networks [3]. There is a need for a mechanism in a distributed environment with self-organizing capability.

A different localized algorithm, namely, Efficient Distributed Detection (EDD) algorithm has been proposed in the earlier works. In the EDD method, each node communicates only with its one- hop neighbors. This characteristic of EDD not only reduces the communication overhead, but also protects them from node compromise. However, the detection accuracy is low when the number of replicas increases.

The main aim of the proposed work is to increase the level of accuracy in detection with minimum overheads during the replica node detection in sensor networks. To achieve this, the existing localized EDD algorithm is enhanced.

This paper is organized as follows: In Section 2, the earlier works done in the problem domain are discussed. Section 3 discusses the proposed methodology- the enhanced EDD. Section 4 discusses the experimental setup and the results due to experimentation. Section 5 concludes the paper.

2. Review of Literature

Detection of clone attacks in mobile WSN is a challenging task under hostile environment. The existing clone detection methods are either centralized or distributed. The centralized detection methods have limitations which include single point failure and the sensor nodes can be easily captured and replicated by the adversary. Therefore, distributed detection methods are proposed in the literature and they are discussed below:

Ho et al [7] in 2009 follows predetermined zone approach and actually deployed zone distance measure to detect replicas by fixing distance thresholds. In this method, if a genuine node is erroneously located in a zone beyond the threshold distance, it may yield a detection error by determining it as a replica.

Jun-Won et al [5] in 2011 introduced a fast and effective mobile replica node detection scheme by the Sequential Probability Ratio Test. This is the foremost algorithm to tackle the problem of replica node attacks in mobile sensor networks.

Conti et al [9] in 2011 uses a distributed algorithm for replica detection in the two-dimensional mobility model. In the two dimensional mobility models, the nodes are uniformly and randomly placed in the network at the beginning of each round. The advantage of this method is that the position of each node is independent of the one in the previous round. In this algorithm, each node maintains a list of node IDs, time, and the locations it encountered in the past time units. The information about every move of a node is broadcasted to its neighboring nodes. This helps the nodes to verify whether there is a node appearing in two distant locations at the same time.

Ho et al in [6] 2012 used a statistical decision process to detect replicas with multiple pieces of evidence. In this method, base station uses the evidence to find whether a suspected node is a replica or not.

Yu et al [11] in 2013 use a distributed algorithm, namely the extremely Efficient

Distribution (XED) method that detects the replica based on the random number they exchange when two nodes meet each other. The detection capability is degraded when the replicas exchange the exact random value.

Yu et al [11] in 2013 utilizes the Efficient Distribution Detection method to detect node replication attack in the distributed environment. This method not only balances the overheads but also avoids network- wide time synchronization and also network- wide revocation. Table 1 presents the significant clone detection methods available in the literature.

The general overheads in the clone detection are communication cost, memory utilization and discovery of node locations. From the literature, it is observed that EDD algorithm has better overheads when compared to other detection methods. However, in the EDD algorithm the false detection rate increases and the detection accuracy decreases when there is an increase in the number of replicas. Hence an attempt is made to improve the existing EDD algorithm in terms of detection accuracy. The proposed work enhances the EDD using Artificial Immune System. The next section discusses the system model of the proposed approach.

Table 1.Comparison of Significant Clone Detection Methods

Year	Authors	Techniques Used	Clone detection mechanisms	Parameters used for evaluation
2009	J.-W. Ho, D. Liu, M. Wright, and S.K. Das	Group Deployment Knowledge	If the node is beyond the threshold distance, yield a detection error by determining it as a replica	Communication overhead, computation overhead and storage overhead
2011	Jun-Won Ho; Wright, M.; Das, S.K.	Sequential Probability Ratio Test	If a node present at different location exceeds the predefined velocity, then the base station detects them as a replica	Number of claims, False Positive and False Negative
2011	M. Conti, R.D. Pietro, L. Mancini, and A. Mei	Two-dimensional mobility model	Detects the clone node when a node appears in two distant locations at the same time	Storage overhead and Memory overhead
2012	J.-W. Ho, D. Liu, M. Wright, and S.K. Das	Statistical decision process	Detect replicas with multiple pieces of evidence	Number of reports, False Positive and False Negative
2013	C. M. Yu, Y. T. Tsou, C. S. Lu, S. Y. Kuo	eXtremely Efficient Detection	Detects replica based on the random value exchanged between the two meeting nodes	Detection accuracy, Detection time, Storage Overhead, Computation Overhead, Communication Overhead
2013	C. M. Yu, Y. T. Tsou, C. S. Lu, S. Y. Kuo	Efficient Distributed Detection	When a node exceeds the pre- defined threshold value, then it is detected as a replica	Detection accuracy, Detection time, Storage Overhead, Computation Overhead, Communication Overhead

3. System Model

This section explains the Mobile Wireless Sensor Network model and the adversary model. Two important models considered in the proposed approach are the network model and the threat model.

3.1. Network Model

The wireless sensor network contains the number of sensor nodes with a unique identity ID from 1 to n and follows symmetric communication as shown in Figure 1. Each node in the network sends beacon message periodically, which contains (ID, neighbor ID) and maintains equal time intervals. The sensor nodes use Random Way Point (RWP) mobility model for its mobility [12, 13, 14].

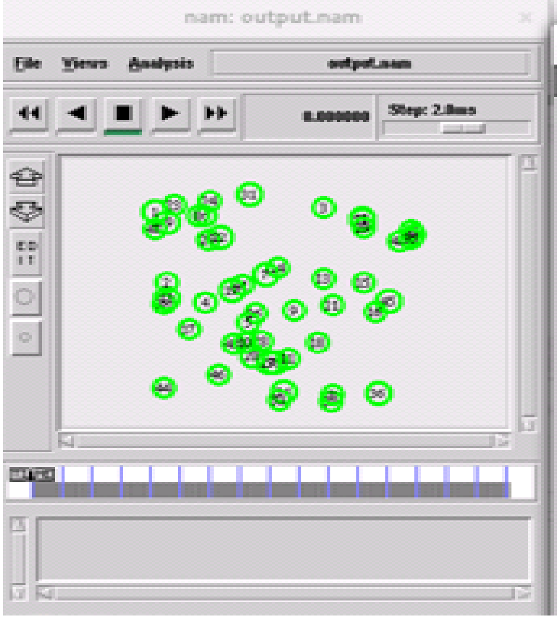


Figure 1. Network Model

Each node will be aware of its geographic position. Each node in the sensing field moves towards the destination point with its speed in a predefined interval randomly. If the node reaches the destination point, node continues to remain static for random time. Then it follows the same mobility rule again. To minimize the complexity, each node has k average neighbors per each move in the network. The network uses identity-based public key system [15, 16].

3.2 Threat Model

Nodes in the sensor network are not tamper resistant. Replica node can be accessed with the help of the node's legitimate security credentials that are acquired by compromising the sensor node immediately at every sensor deployment. After gaining the access, the adversary deploys one or more node with the same ID. This is called Replica node. Replica nodes can communicate, collude with each other and remain silent for a particular time after the collusion in order to avoid replica detection in EDD. The threat model is depicted in Figure 2.

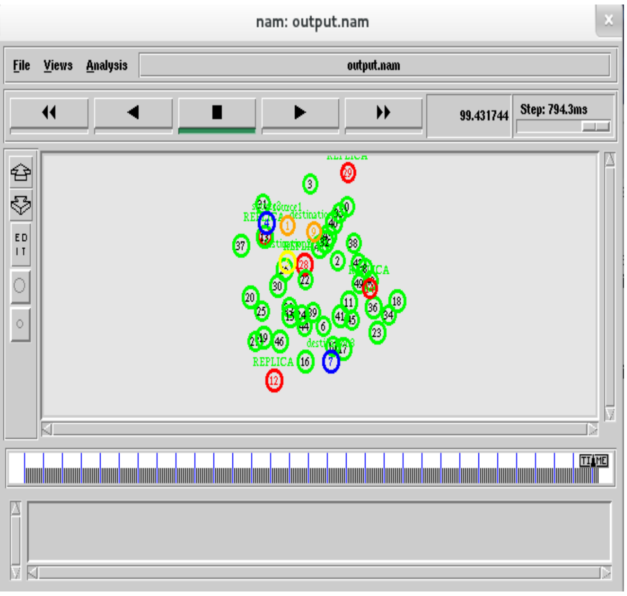


Figure 2.Threat Model

Based on the mobile wireless sensor network model and the threat model, the proposed Enhanced EDD (EEDD) is developed.

4. Proposed Methodology

The proposed work enhances the EDD method by combining the Danger Theory to detect the replica node in mobile WSN. The EDD method is one of the node meeting based detection method in which the detection is by comparing the threshold value with the number of encounters. A threshold value is initially assumed based on the node's communication. Danger theory immune inspired algorithm is based on Received Signal Strength of mobile node. Enhanced EDD with Danger theory is explained below.

4.1. Enhanced EDD with Danger Theory

In the EDD method, the detection method consists of both the online step and the offline step. Offline and online steps are used before and after the deployment respectively. In the offline step, the time interval length and the threshold value are computed to identify the replica node. In the online step, each node in the network identifies whether the node is a replica or not by comparing the calculated threshold with the number of times the node is encountered. The detail of these two methods is described below.

4.2. Offline Step

The array L (i.e L (1) to L (n)) is used to maintain the number of times the node is encountered with another node in a given time interval length T and the array D (i.e D (1) to D (n)) contains the ID of the replica node in the network. $\mu_1$and$\mu_2$are used to calculate the expected number of genuine and replica node. σ_1^2andσ_2^2 are used to calculate the variance of the genuine node and the replica node.

The maximum number of times a genuine node encountered is denoted as Y1 and the possibility of minimum number of times the replica node encountered with every other node is denoted as Y2 and are computed [11]as,

$$Y1 = \mu_1 + 3\sigma_1 \qquad (1)$$

$$Y2 = \mu_2 + 3\sigma_2 \qquad (2)$$

Threshold,φ can be computed as,

$$\varphi = \frac{Y2-Y1}{2} \qquad (3)$$

If the number of times the node encountered is greater than the threshold, then the node is called as replica node. This replica ID is stored in array D.

4.3 Calculation of $\boldsymbol{\sigma_1^2}$ and $\boldsymbol{\mu_1}$

Let us establish the location of the sensor nodes and the corresponding communication disk of range r. Let us consider a mobile sensor node. The distribution of the number of times a particular node resides over the communication disk of the static node is derived and this act as the distribution of the number of encounters with a genuine node. The calculation of $\boldsymbol{\sigma_1^2}$ and μ_1 are done from the derived distribution.

Let us assume that the time interval of length T, X^{th}moving node takes $\tau(T)$ steps. Let, the length of k-th step be l_k . The length is the distance between the current position of the X^{th}node, $P_{i-1}$and randomly selected destination position, P_i.The time taken by the k-th step is

$$t_k = \frac{l_k}{v} + b \qquad (4)$$

The mean (μ) and variance (σ) are derived as,

$$\mathrm{E}\,[t_k] = E\left[\frac{l_k}{v} + b\right] = \left(\mathrm{E}\frac{[t_k]}{v}\right) + b \qquad (5)$$

and

$$\mathrm{E}\,[{t_k}^2] = \mathrm{E}\,\left[\frac{l_k}{v} + b^2\right] = \left(\frac{\mathrm{E}[{l_k}^2]}{v^2}\right) + \left(\left(\frac{2\mathrm{b}}{\mathrm{v}}\right) * \mathrm{E}[l_k]\right) + b^2 \qquad (6)$$

Where ‘v’ is the constant velocity and ‘b’ is the constant time.
Variance of t_k is derived [11] as

$$\text{Variance}\,[{t_k}^2] = \left(\mathrm{E}\frac{[{l_k}^2]}{v^2}\right) + \left(\left(\frac{2\mathrm{b}}{\mathrm{v}}\right) * \mathrm{E}\,[l_k]\right) + b^2 - (E[l_k]/v + b)^2 \qquad (7)$$

Hence $\tau(T)$ [11] can be defined as

$$\tau(T) = \max\{m{:}\, A_m \le T\}\text{where}A\_(m\ \ ) = ∑\_(K = 1)\text{^}m\ t\_k \qquad (8)$$

where$A$ * A is the size of the sensing region in the network. Using the same method, the parameters $\mu_2$and σ_2^2 are calculated.

4.4 Online Method

Sensor nodes in the network keep the counter ‘t’ to record the time at the beginning of each time interval. If the time interval ‘t’ exceeds threshold, reset the counter t=0. A node x in the network meets another node in a network at every time ‘t’ value of the array L is incremented by 1. If node x meets y node more than the threshold φ, node y can be added to the array D for further process.

To enhance the performance of the existing EDD method, the danger theory of AIS is applied. Danger theory algorithm is an important algorithm in AIS. In order to deal with node replication attack Danger Theory Immune Inspired Intrusion Detection System is adopted to enhance the EDD method to obtain better detection rate. The Danger theory ejects danger signals when antigens are present in the body. Dendritic cells (DC) play a vital role in detecting and processing different types of signals which includes danger signal too. Using DCs, the attacks can be detected in the network. The logical architecture of Danger theory inspired IDS is shown in Figure.3. It consists of three phases, namely

- Collection Phase
- Analysis Phase
- Decision Phase

The collection and the analysis phase are carried out using the Dendritic cell algorithm (DCA) whereas the decision phase is carried out using the decision taking procedures of the lymph node. The DCA performs three operations like initialization, updation and aggregation. The parameters of the algorithm are organized and initialized and the DCs are referred to the immature state during initialization. The antigens and the corresponding signals are updated during updation and the state of the DC is changed to semi- mature (self) or mature (non- self) in the output of this process. In the aggregation phase, the DCs and their states received are given as input for determining the behavior of the antigens. The phases are explained below:

4.5 Collection Phase

The monitoring component is the principal component of the collection phase that is responsible for collecting the antigens from the array D and the corresponding signals. The antigens contain the information about the total number of sent and received messages of the suspected non-self-node. The signals correspond to the Received Signal Strength Information (RSSI) of the suspected non-self-nodes. These parameters are mainly used to determine the possible intrusions.

4.6 Analysis Phase

The Intrusion Detection manager is the central component which analyzes the information collected from the monitored component from which decision will be taken by next phase. This information contains the behavior of the non-self-node. IDS manager acts the role of coordinating tasks, actions and responses behalf of another manager in the subsystem. Upon receiving the attack from the IDS, the IDS manager directs it to the Context Manager about the attacks that are observed by the intrusion detection system and seek the Parameters Base for the parameters that need to be observed by the Monitoring component. The Monitoring component periodically captures the information from the parameter Base and it uses the following utility function [10] to generate the output signals. The monitored components use the utility function [10] in order to determine the output as,

$$Output\begin{bmatrix} CSM \\ Mature \\ Semi-mature \end{bmatrix} = \left(W_P \sum_{i=0}^{I} P_i + W_D \sum_{i=0}^{I} D_i + W_S \sum_{i=0}^{I} S_i\right) \times (1+IC) \quad (9)$$

where, P_i denotes the PAMP signal, D_i represents the danger signal and S_i denotes the Secure Signal. W_P, W_D and $W_S$are the corresponding weights. The maturation state of the DC is the output of the equation (9).When the replica node is present, then the DC will be mature or else it will be in the semi- mature state. The monitoring component routes the current measures to the context manager and then the context manager is sent by the intrusion detection manager to the decision manager.

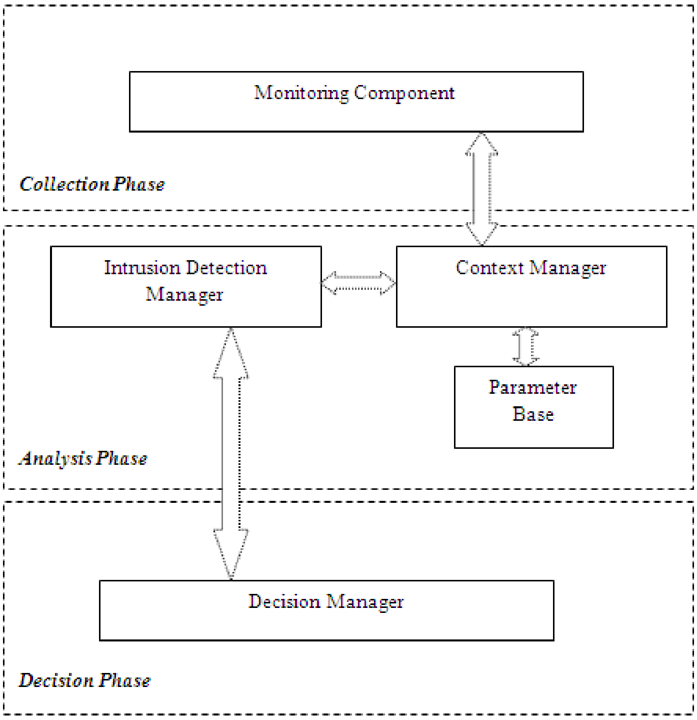


Figure 3. IDS Logical Architecture

4.7 Decision Phase

The decision phase takes place in the lymph node and it is accomplished using the decision manager. The Decision Manager receives the information from the intrusion detection manager to find the possibility of attacks in the sensor network. If the node has maximum RSS, then check the previous communication of that node. If the node has earlier communication, then it is called self-node. The node that has the low RSS value is termed as a replica. Once replica attack is identified, the Intrusion Detection Manager is warned.

Pseudo Code for Danger Theory Inspired AIS

```
Collect the non- self node behavior
    Analyze the behavior of the node by Intrusion Detection Manager
        Decide the nodes behavior based on the Receiver Signal Strength received from the node
            Check whether the signal strength is maximum
        If (max)
        Check previous communication for non-self node
            If (Communicates)
                Declare as Self Node
            Else
        Declare as replica node
            End if
        Else
        Declare Minimum signal strength node as replica node
```

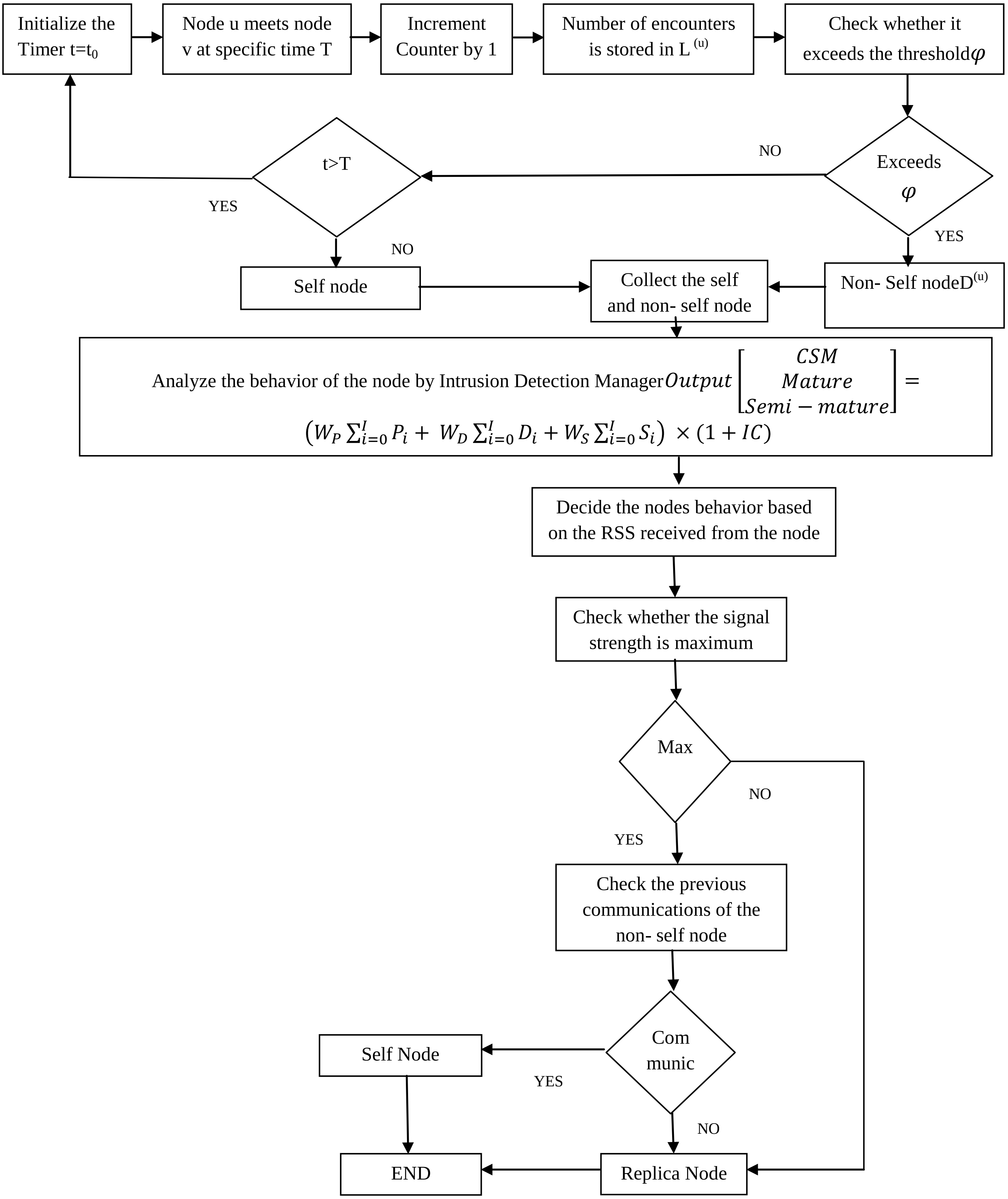

Initialize the Timer $t=t_0$
Node u meets node v at specific time T
Increment Counter by 1
Number of encounters is stored in $L^{(u)}$
Check whether it exceeds the thresholdφ
Exceeds φ
NO
t>T
YES
NO
YES
Self node
Collect the self and non- self node
Non- Self node$D^{(u)}$
Analyze the behavior of the node by Intrusion Detection Manager$Output\begin{bmatrix} CSM \\ Mature \\ Semi-mature \end{bmatrix} = \left(W_P \sum_{i=0}^{I} P_i + W_D \sum_{i=0}^{I} D_i + W_S \sum_{i=0}^{I} S_i\right) \times (1+IC)$
Decide the nodes behavior based on the RSS received from the node
Check whether the signal strength is maximum
Max
NO
YES
Check the previous communications of the non- self node
Com munic
YES
NO
Self Node
END
Replica Node

Figure 4.The Flow Diagram of the Proposed Methodology

Pseudo Code of the Proposed Methodology

```
Input: packet
Declare:  count as C, time as t, Received signal strength as RSS
Output: replica or self node
Algorithm 1
        Initialize the timer t=$t_0$
        If( node u meets node v at specific time t)
            Increment counter c by 1
                Number of encounter stores it in list, $L^{(U)}$ [v]=c
            Check whether it exceeds the threshold
            If ($L^{(U)}$ [v] >$\varphi$)
                Declare node as Non- Self node
                Collect the non- self node behavior in array $D^{(U)}$
              Analyze the behavior of the node by Intrusion Detection Manager
               Decide the nodes behavior based on the Receiver Signal Strength
                   received from the node
                Check whether the signal strength is maximum
                If (max)
                  Check previous communication for non-self node
                  If (Communicates)
                    Declare as Self Node
                  Else
                    Declare as Replica Node
                  End if
                Else
                  Declare Minimum signal strength node as replica node
                End if
            Else
                Declare node as self node
            End if
        Else if (t>T)
            Reset timer t=$t_0$
            Repeat Algorithm 1          End if
```

5. Experimentation and Results

In the experimental analysis, the behavior of nodes in wireless sensor network and its performance are analyzed using enhanced EDD with danger theory. The proposed methodology is implemented using NS-2. It is popular and well known network simulator tool. This tool is used in the area of MANET, wireless sensor network, etc. In this work, the network consists of 50 mobiles nodes and replica nodes. The number of replica nodes is varied with time. The analysis is made in the enhanced EDD with danger theory of AIS. The simulation parameters are used while implementing this proposed technique is summarized below in the Table 2. These parameters are used to construct the network.

Table 2.Simulation Parameters

Simulation Parameter	Value
Propagation	TwoRayGround
Channel	WirelessChannel
Physical Layer	WirelessPhysical
Queue	DropTail/PriQueue
Mac	802_.11
X dimension of the topography	500
Y dimension of the	500
Adhoc Routing	AODV
Antenna	Omni Antenna
Max packet	100 (Minimum:512bytes, Maximum:
No of nodes simulated	60 (Minimum:10nodes, Maximum: 60 nodes)
Cp	./cbr
Sc	nodes50
sSimulation time	200 s(Minimum:200s, Maximum:10000s)
Energy	EnergyModel
Initial Energy	100
aodvMinNeighbor	6
aodvSecurityDuration	4
Aodv Minimum Neighbor	6
No of replica node	5 (Minimum:5, Maximum: 25)
locerrorRef	5
locerrorThr	4

5.1 Evaluation Metrics

The performance of this work is analyzed using the route overhead, packet delivery ratio, energy consumed, location error and average packet delay. The accuracy of detection of replica node is measured using detection ratio and which is represented in Xgraphs. This graph shows efficient results towards the detection and identification of replica nodes in WSN. Overhead 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 (10).

$$Overhead = \frac{data\ packets\ received}{control\ packets\ generated} \qquad (10)$$

Figure 5 shows the graph for routing overhead, which shows that the existing EDD approach has higher routing overhead than proposed Enhanced EDD-danger theory which has lesser routing overhead.Energy is 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 (11).

$$Average\ Energy\ Consumed = \frac{Sum\ of\ percent\ energy\ consumed\ by\ all\ nodes}{Number\ of\ nodes} * joule$$
(11)

The graphs 5,6,7,8,9,10 and 11 shows the performance of the algorithm in terms of routing overhead, energy consumed, packet delivery ratio, average delay, localization errors, detection ratio and false alarm rate. The Figure 6 shows the graph for the energy consumed, which shows that the existing EDD approach has high energy consumption value than proposed Enhanced EDD-danger theory which has high energy consumption value. The energy consumed is represented by joule (J).

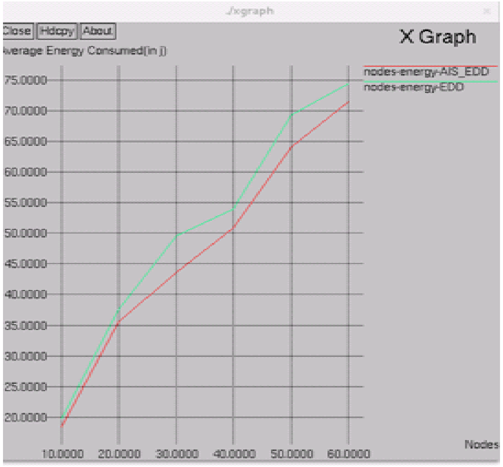


Figure 5.Routing Overhead

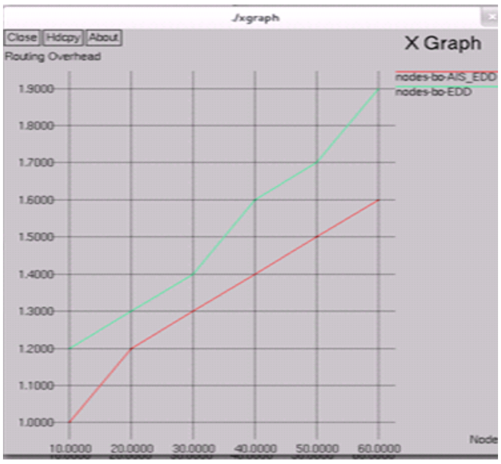


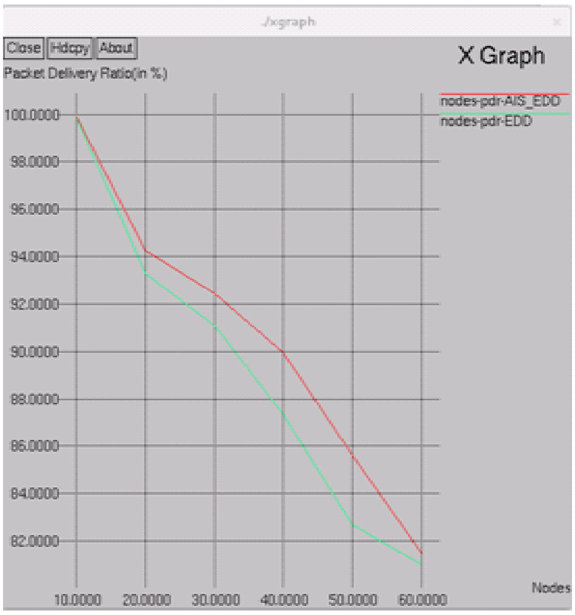
Figure 6.Energy Consumed

Packet Delivery Ratio (PDR) is 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 (12).

$$PDR = \frac{received\ packets}{sent\ packets} * 100 \qquad (12)$$

Figure 7 shows the packet delivery ratio, which shows that the existing EDD approach have a lower packet delivery than proposed Enhanced EDD-danger theory which has higher a packet delivery ratio. The packet delivery ratio is represented by the percentage (%).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 (13). The parameter is measured only when the data transmission has been successful.

$$Average\ Delay = \frac{Sum\ of\ all\ packets\ delay}{Total\ Number\ of\ Received\ Packets} \qquad (13)$$



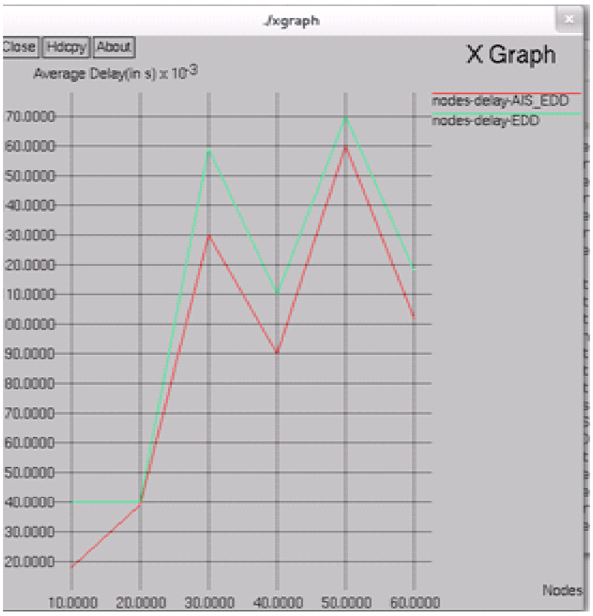
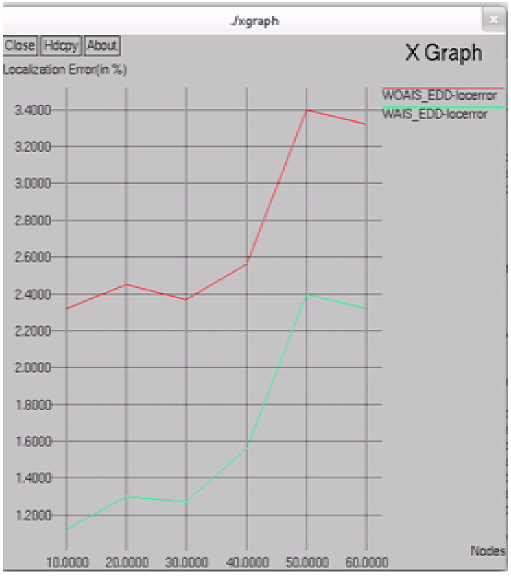


Figure 6. Packet Delivery Ratio

Figure 5.Average Delay

Figure 7 shows the graph for average packet delay which shows that the existing EDD approach has a higher packet delay than proposed Enhanced EDD-danger theory which has low packet delay. The average delay is represented by seconds (s). The Figure 9 shows the graph for Localization error which shows that the existing EDD approach has higher location error than proposed Enhanced EDD-danger theory. It is represented by percentage (%).



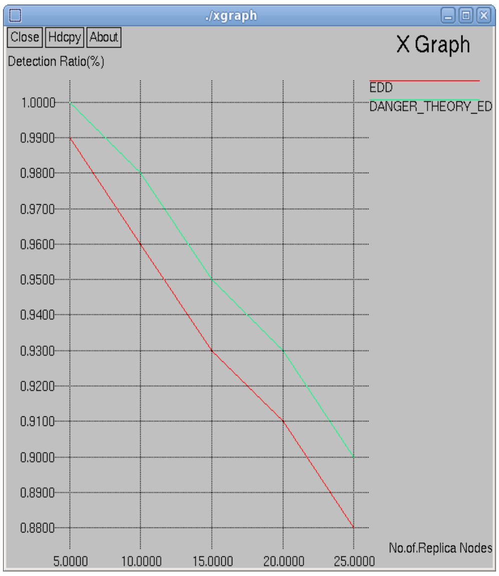


Figure 7.Localization Errors

Figure 8.Detection Ratio

Detection ratio is defined as Number of replica node correctly found by Total number of replica node. It is represented by percentage (%).

$$Detection\ Ratio = \frac{Number\ of\ Replica\ nodes\ Correctly\ found}{Total\ Number\ of\ Replica\ Nodes} * 100 \qquad (14)$$

Figure 10 shows the graph for Detection ratio which shows that existing EDD approach has a lower detection rate than proposed Enhanced EDD-danger theory. It is represented by percentage (%).False alarm rate is defined as Number of replica node correctly found by Total number of replica node. It is represented by percentage (%).

$$False\ Alarm\ Rate = \frac{Total\ Number\ of\ Replica\ Node - Number\ of\ replica\ node\ correctly\ found}{Total\ Number\ of\ Replica\ Node} * 100 \qquad (15)$$

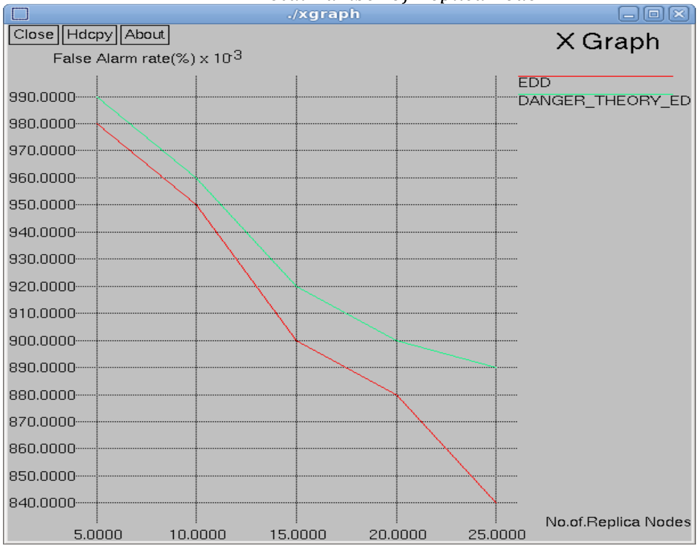


Figure 9. False Alarm Rate

Figure 11 shows the graph for false alarm rate, which shows that the existing EDD approach has a higher false alarm rate than proposed Enhanced EDD-danger theory. It is represented by percentage (%). The performance of the proposed method with the existing method by varying the number of nodes is given in Table 3.

Table 3.Performance of Proposed Method and the Existing Method Based on the Number of Nodes

No of Nodes	Routing Overhead (kbps)		Energy Consumed (J)		Packet Delivery Ratio (%)		Average Delay (s * 10^{-3})		Localization Error (%)	
	EDD	EEDD	EDD	EEDD	EDD	EEDD	EDD	EEDD	EDD	EEDD
10	12000	10000	20.0000	19.5000	99.0000	100.0000	40.0000	20.0000	2.3000	1.1000
20	13000	12000	37.5000	35.0000	93.0000	94.7500	40.0000	40.0000	2.4500	1.3000
30	14000	13000	50.0000	44.0000	91.5000	92.2500	40.0000	30.0000	2.3950	1.2750
40	16000	14000	54.0000	51.0000	88.7500	90.0000	10.0000	90.0000	2.5750	1.6000
50	17000	15000	70.0000	64.0000	82.2500	84.9500	70.0000	60.0000	3.4000	2.4000
60	19000	16000	74.0000	71.0000	81.0000	81.9500	20.0000	00.5000	3.3000	2.3000
Average	15166.67	13333.33	50.9166	47.4166	89.2500	90.6500	36.6666	40.0833	2.7366	1.6625

The performance of the proposed method with that of the existing method by varying the number of replica nodes is given in Table 4.

Table 4. Performance of proposed and the existing based on the number of replicas

No of Replica Nodes	Detection Ratio (%)		False Alarm Rate (%) * 10^{-3}	
	EDD	EEDD	EDD	EEDD
5	0.9900	1.0000	98.0000	99.0000
10	0.9600	0.9800	95.0000	96.0000
15	0.9300	0.9500	90.0000	92.0000
20	0.9100	0.9300	88.0000	90.0000
25	0.8800	0.9000	84.0000	89.0000
Average	0.934	0.952	91.0000	93.2000

The overall comparison results of this work are shown in the Table 5 below.

Table 5. Comparison Result

Metrics	Existing EDD (kbps)	Proposed Enhanced EDD (kbps)	Improvement (%)
Routing overhead	19,000	16,000	3
Energy consumed (joule)	7,40,000	7,10,000	0.3
Packet delay(sec)	40.000	20.000	20
Packet delivery ratio (%)	99.0000	100.0000	1.0
Localization error (%)	3.3000	2.3000	10
Detection ratio(%)	0.9900	1.0000	10
False detection ratio (%)	98.0000	99.0000	10

The above Table 5 clearly shows the percentage of improvement achieved for various performance metrics of the proposed technique Enhanced EDD (EEDD) while comparing with existing EDD. The proposed work improves its performance in all the metrics, where the detection ratio is improved much better than EDD.

6. Conclusion

In a wireless sensor network, security is the main issue. This paper is mainly focused on the node replica attack. Various replica detection methods are used to mitigate node replication attack. They undergo network degradation when multiple replicas are involved. The proposed replica detection method protects the network from multiple replica nodes. The proposed enhanced EDD (EEDD) with danger theory of Artificial Immune System is energy efficient with reduced overhead and low false alarm rate is suitable for the deployment of sensor nodes for identifying replica nodes. The experimental analysis of proposed Enhanced EDD (EEDD) is compared with existing EDD and the results shows that average delay, energy, overhead and message drops are minimum with higher PDR value and higher detection ratio.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, **(2002)**, pp. 102–114.

[2] D. Puccinelli and M. Haenggi, “Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing”, IEEE Circuits and Systems Magazine, **(2005)**.

[3] K. Xing and X. Cheng, “From time domain to space domain: Detecting replica attacks in mobile ad hoc networks”, Proc. IEEE Int. Conf. Computer Communications (INFOCOM), **(2010)**; San Diego, CA, USA.

[4] B. Parno, A. Perrig and V. D. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks”, Proc. IEEE Symp. Security and Privacy, **(2005)**.

[5] J. W. Ho, M. Wright and S. K. Das, “Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing”, Mobile Computing, IEEE Transactions on Mobile Computing, vol. 10, no. 6, **(2011)**, pp. 767-782.

[6] J. W. Ho, M. Wright and S. K. Das, “Zonetrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing”, IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, **(2012)**, pp. 494-510.

[7] J. W. Ho, D. Liu, M. Wright and S. K. Das, “Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks”, J. Ad Hoc Networks, vol. 7, no. 8, **(2009)**, pp1476-1488.

[8] Z. Bo, V. G. K. Addada, S. Setia, S. Jajodia and S. Roy, “Efficient Distributed Detection of Node Replication Attacks in Sensor Networks”, Computer Security Applications Conference, ACSAC, Twenty-Third Annual, **(2007)**.

[9] M. Conti, R. D. Pietro, L. Mancini and A. Mei, “Distributed Detection of Clone Attacks in Wireless Sensor Networks”, IEEE Trans. Dependable and Secure Computing, vol. 8, no. 5, **(2011)**, pp. 685-698.

[10] H. M. Salmon, C. M. Farias, P. Loureiro, L. Pirmez, S. Rossetto, P. H. Rodrigeus, R. Pirmez, F. C. Delicato and L. Fernando, “Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune- Inspired Techniques”, Int. Journal of Wireless Inf. Networks, Springer, vol. 20, **(2012)**, pp. 39-66.

[11] Y. C. Mu, T. Y. Tung, L. C. Shien and K. S. Yen, “Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks”, IEEE Trans. information forensics and security, vol. 8, no. 5, **(2013)**, pp.754-768.

[12] D. B. Johnson and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks”, Mobile Computing, **(1996)**, pp. 153–181.

[13] J. Yi, J. Koo and H. Cha, “A localization technique for mobile sensor networks using archived anchor information”, Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), **(2008)**; California, USA.

[14] L. Zhou, J. Ni and C. V. Ravishankar, “Supporting secure communication and data collection in mobile sensor networks”, IEEE Int. Conf. Compute Communications (INFOCOM), **(2006)**; Barcelona, Spain.

[15] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks”, Int. Conf. Information Processing in Sensor Networks (IPSN), **(2008)**; Missouri, USA.

[16] D. J. Malan, M. Welsh and M. D. Smith, “Implementing public-key infrastructure for sensor networks”, ACM Trans. Sensor Network, vol. 4, no. 4, **(2008)**, pp. 1–23.

Authors

L. S. Sindhuja is pursuing her Ph. D at Avinashilingam University for women, Coimbatore. She has 2 years of teaching experience. Her areas of interest include Network and Communication Security. She has 5 publications in her research area.

G. Padmavathi is the Professor and Head, Department of Computer Science, Avinashilingam University for women, Coimbatore. She has 25 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication,Network Security and Cryptography. She has more than 100 publications in her research area. Presently, she is guiding M.phil researchers and Ph.D Scholars .She has been profiled in various organizations for her academic contributions. She has been the Principal Investigator of four projects funded by UGC and DRDO and Scientific Mentor for one project funded by DST. She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.