Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

An improved efficient distributed detection algorithm in wireless sensor networks

Xiaolong Xu *

Experiment Teaching Center, Qufu Normal University, Rizhao Shandong, China.

Global Journal of Engineering and Technology Advances, 2026, 27(02), 185–194

Publication history: Received on 18 April 2026; revised on 24 May 2026; accepted on 26 May 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.27.2.0133

Abstract

In wireless sensor networks, attackers can capture the security certificate of some nodes and reproduce a large number of nodes with the same identity. Replica nodes have all the permissions of legitimate nodes and attackers can use them to carry out a variety of attacks. To solve this problem, we proposed the improved efficient distributed detection (IEDD) algorithm. It combines the EDD algorithm with the artificial immune algorithm to detect the node replication attack and can prevent replica nodes appear in wireless sensor networks. Simulation results show that this method can reduce energy consumption, shorten time delay, improve detection rate and packet delivery ratio.

Keywords: Wireless Sensor Network; Node Replication Attack; Attack Detection; Immune Algorithm

1. Introduction

In recent years, wireless sensor networks have been widely used in sensing mobile nodes and wireless communication, sensor networks can be used in many fields, such as medical, military, environmental monitoring and so on. Compared with Ad Hoc network, the sensor network is characterized by a large number of nodes and more intensive deployment to ensure coverage and connectivity. In wireless sensor networks, tens of thousands of nodes share and process information through the wireless channel, and the tiny sensor nodes that participate in communication have the ability of sensing and data processing. Due to this, the wireless sensor network is vulnerable to various attacks in the communication process. Replica node attacks are very dangerous; the attacker can capture the key and ID from the attacked node and replicate in the network [1]. These replica nodes communicate using software and the information captured from the compromised nodes. The attacker who controlled the replica nodes can act as authorized nodes. Communication protocol allows replica nodes to create shared keys, so that the replica nodes can encrypt, decrypt, verify all communications, just like real nodes [2].

A variety of attack detection methods proposed in many literatures can effectively detect attacks only under stable conditions. However, in many applications, the sensor nodes can only communicate on the unreliable and unstable media [3]. According to the needs of applications, they can only use limited resources for communication. The existing centralized mechanisms can not only fail in the unstable environment, but also is not suitable for the applications using restricted resources [4].

In literature [5], the EDD (Efficient Distribution Detection) method is used to detect node replication attacks in distributed environment. This method not only can balance the overhead, but also can avoid the time synchronization and code revocation. However, when the number of replica nodes increases, the false detection rate of EDD algorithm is increased, and the detection accuracy is decreased. So, we try to improve the detection accuracy of the existing EDD algorithm. The proposed approach uses artificial immune systems to enhance the performance of the EDD algorithm. The system model of the proposed scheme will be discussed in the next chapter.

* Corresponding author: Xiaolong Xu

This paper is organized as follows: Chapter 1 discusses the early work in this field. Network model and threat model of wireless sensor networks are introduced in chapter 2. In chapter 3, the proposed IEDD method is discussed. Experimental setting and experimental results are discussed in chapter 4. Chapter 5 makes a summary of the whole paper.

2. Literature Review

Replica attack detection in wireless sensor networks is a challenging task. The existing replica detection methods are divided into centralized detection and distributed detection. The main limitations of centralized detection methods include single point failure and sensor nodes can be easily captured and copied by attackers. So, the distributed detection algorithm is proposed in many literatures.

Three distinctive algorithms were proposed in literature [6], which showed good performance in detection rate, system overhead, and other aspects.

Literature [7] looks at the Multi Area Method (MAA) Replica Identification with Deployment with Location Knowledge (DLK) used. Based on the deployment performance, this model is compared to Area Based Cluster move towards (ABCD) and Fingerprint-based detection techniques. The proposed methodology offers excellent performance compared with other standard methods.

Literature [8] proposed FEC approach. In the traditional method, the replica node is detected by the parameter's mobility speed, node id and energy. The parameters used in the existing system is not able to detect the exact replica node. The proposed approach (FEC) overcame the issues of existing system, offered high detection rate and minimal communication overhead.

3. System Model

This chapter introduces the mobile wireless sensor network model and the attacker model. The two important models considered in the proposed scheme are network model and threat model.

3.1. Network Model

The sensor nodes in wireless sensor networks have a unique ID, numbered from 1 to N, they can carry out symmetrical communication. Each node in the network periodically sends beacon messages, which contain ID, adjacent nodes ID, and maintain equal time intervals. Sensor nodes use RWP (Random Way Point) mobile model to move. Each node is aware of its location, nodes in the sensor area move to the target position with their own speed at a predetermined time interval. If a node reaches its destination, the node remains stationary for a period of time, and then moves in accordance with the same rules. In order to reduce the complexity, each node in the network has an average of k neighbors. The network uses identity-based public key cryptosystem.

3.2. Threat Model

Nodes in the sensor network don't have the ability to prevent tampering. The replica nodes can access network using the valid security certificate obtained at the time of deployment. If access is gained, the attacker deploys one or more nodes with the same ID, which is replica nodes. Replica nodes can communicate with each other, and keep silent for a certain period of time after the communication to avoid a replica detection of the EDD algorithm. Based on the wireless sensor network model and threat model, we propose the IEDD algorithm.

4. The Proposed Method

The proposed method combines the danger theory of the artificial immune system to enhance the performance of the EDD algorithm. EDD algorithm is a detection method based on node encounter, it compares the encounter times with the threshold to detect, the threshold is set based on the node's communication. The danger theory of immune algorithm is based on the strength of the signal received by the mobile node.

4.1. The Improved EDD Algorithm Based on Danger Theory

In EDD algorithm, the detection method is composed of online steps and offline steps. The offline and online steps are used before and after the deployment. The time interval length and the threshold are calculated in the off-line step to

determine replica nodes. In the online step, it can determine whether a node is a replica node by comparing the threshold with the times of encounters.

4.2. Offline Step

Array L is used to store the times this node encountered another node in a given time interval T. Array D is used to store replica nodes' ID. μ_1 and μ_2 represent the expected number of real nodes and replica nodes respectively. σ_1^2 and σ_2^2 are used to calculate the variance of real nodes and replica nodes.

The maximum number of times the real node encountered is denoted as Y1, the minimum times of replica node encountered every other node is denoted as Y2, the calculation method is (Yu, Tsou, Lu & Kuo, 2013)

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

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

The calculation method for threshold φ is

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

If the times that a node encountered is greater than the threshold, the node is considered to be a replica node. The ID of the replica nodes is stored in array D.

The Calculation of σ_1^2 and μ_1

Let's set up the position of the sensor nodes and the corresponding communication disk of the range r. The distribution of the times that a particular node resides on a static node communication disk is derived, this is the distribution of the times of encountering real nodes. The calculation of σ_1^2 and μ_1 is done by the derived distribution. Assuming that in the time interval T, the Xth node moves $\tau(T)$ steps. The length of step k is denoted as l_k, the length is the distance between the Xth node's current position P_{i-1} and the random selected end position P_i. The time required for step k is:

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

The mean μ and variance σ is

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

and

$$E[t_k^2] = E\left[\frac{l_k}{v} + b^2 \right] = \left(\frac{E\left[l_k^2\right]}{v^2} \right) + \left(\left(\frac{2b}{v} \right) \times E\left[l_k\right] \right) + b^2 \quad (6)$$

Where v is a constant speed and b is a constant time.

The variance of t_k is

$$Variance\left[t_k^2\right]=\left(E\frac{\left[l_k^2\right]}{v^2}\right)+\left(\left(\frac{2b}{v}\right)\times E\left[l_k\right]\right)+b^2-\left(\frac{E\left[l_k\right]}{v}+b\right)^2 \quad (7)$$

So $\tau(T)$ can be defined as

$$\tau(T)=\max\{m:A_m\le T\} \quad (8)$$

A×A is the size of the sensing area in the network. The same method can be used to calculate the parameters of μ_2 hand σ_2^2.

4.3. Online Step

Sensor nodes use counter t to record time at the start of each time interval. If the time interval t exceeds the threshold, the t will be set to 0. Every time node x encounters another node in time t, the value of array L will increase 1. If the times node x encounters node y exceeds the threshold φ, Node y is added to array D for further processing.

In order to improve the performance of the existing EDD algorithm, we combined the danger theory of artificial immune system. Danger theory is an important algorithm in artificial immune system. In order to deal with node replication attack, intrusion detection system based on danger theory is introduced to enhance the performance of EDD algorithm, which can obtain higher detection rate. When the antigen appears in the body, the danger theory sends out a danger signal. Dendritic cells play a critical role in detecting and processing different types of signals, including danger signals. Using dendritic cells, the network attack can be detected. The logic structure of intrusion detection system based on danger theory is shown in Figure 3.

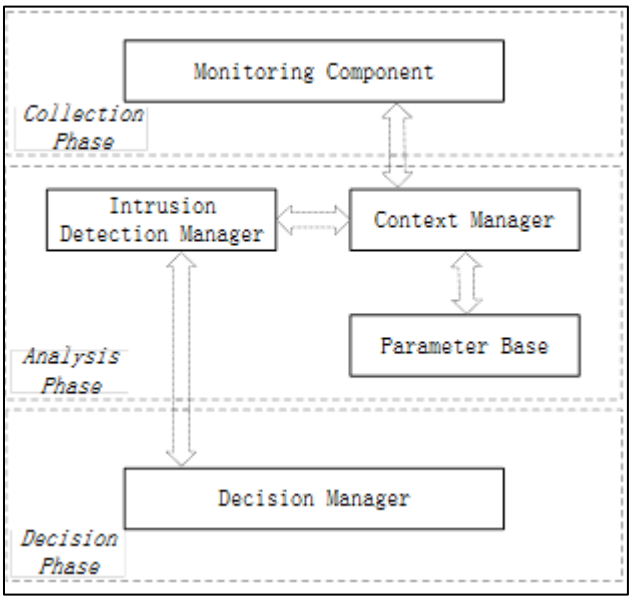

Figure 1 Logical Structure of the IDS

It consists of three phases, respectively

- Collection Phase
- Analysis Phase
- Decision Phase

Collection and analysis phase using dendritic cell algorithm, and decision phase using lymph node decision procedure. The dendritic cell algorithm performs three operations: initialization, update and aggregation. The parameters of the algorithm are organized and initialized, and the dendritic cells are in an immature state during the initial period. The

antigen and the corresponding signal are updated during the update, The state of dendritic cells is changed to semi-mature or mature state. In the aggregation phase, dendritic cells and their states are used as inputs to determine the behavior of the antigens. The following is the interpretation of these phases:

4.4. Collection Phase

The monitoring component is the main component of the collection phase, mainly responsible for the collection of antigens from the array D and the corresponding signals. The antigen contains information about the total number of messages sent and received by a suspected mature node; these signals correspond to the received signal strength information of the suspicious mature nodes. These parameters are mainly used to determine possible intrusions.

4.5. Analysis Phase

Intrusion detection manager is a core component, it analyzes the information collected from the monitoring component to help the decision-making of the next phase, this information contains the behavior of mature nodes. The intrusion detection manager acts as a coordinating role; it's action and behavior represent another manager in the subsystem. Once received attack information from the intrusion detection system, the intrusion detection manager imports it to the context manager of the observed attack, and search the parameter library to find parameters needed to be monitored by monitoring component. The monitoring component periodically captures the information from the parameter library and uses the following utility function to generate the output signal (Conti, Pietro, Mancini & Mei, 2010). The monitoring component uses a utility function to determine the output.

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

Where P_i represents PAMP signal, D_i represents the danger signal, S_i represents safety signal. W_P, W_D and W_s is the corresponding weight. The maturation state of dendritic cells is the output of equation (9). When the replica node appears, the dendritic cells will be in a mature or semi-mature state. The monitoring component transmits the current information to the context manager, and then the context manager is sent to the decision manager.

4.6. Decision Phase

Decision phase is done by using a decision manager in the lymph nodes. Decision manager receives information from the intrusion detection manager to discover possible attacks in sensor networks. If the node has the maximum RSSI, then check the previous communication of the node. If the node has early communications, it is called a semi-mature node. The node with a low RSSI value is called a replica node. As soon as a replica attack is found, the intrusion detection manager will receive an alert.

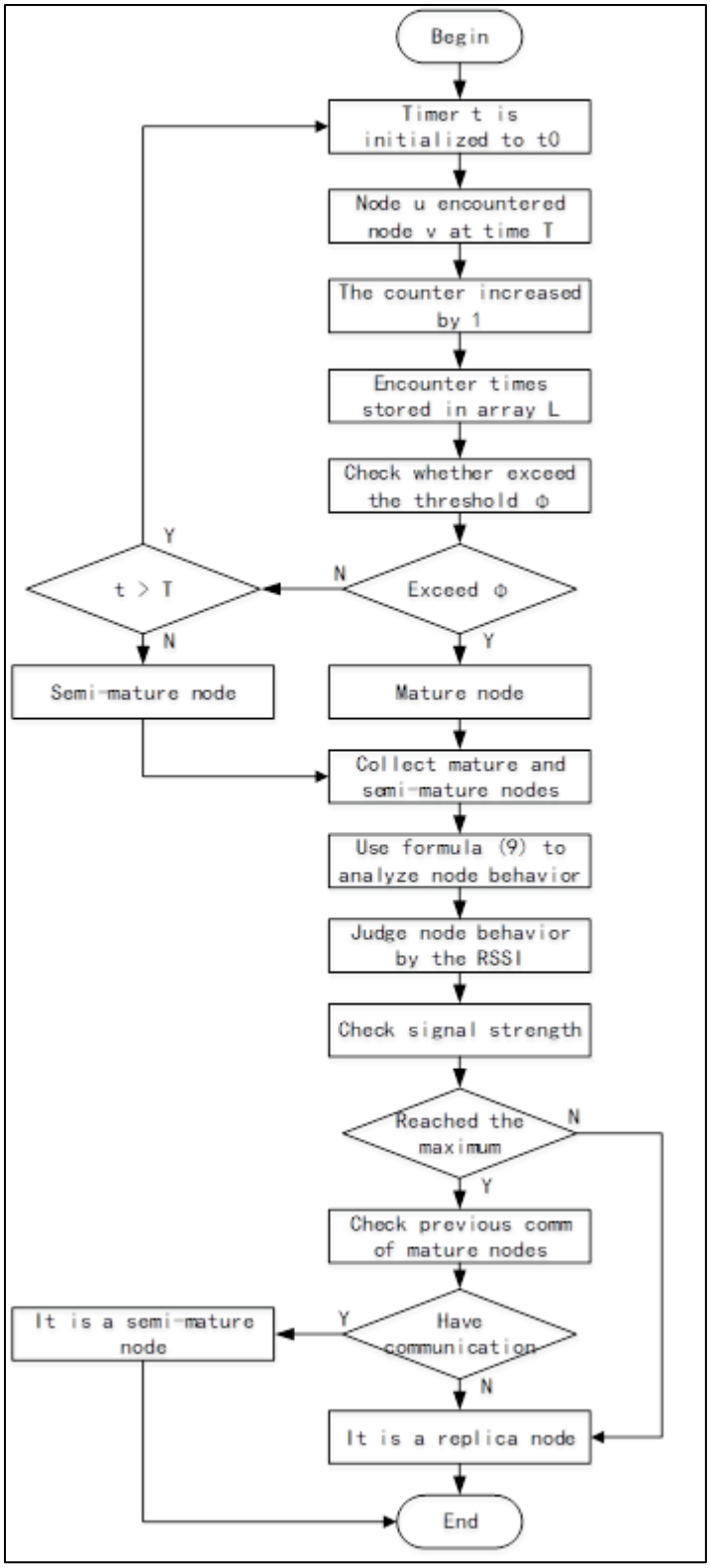

Figure 2 Flow Chart of the Scheme

5. Experiment and Results

In the experimental study, the behavior of nodes in wireless sensor networks and their performance are analyzed by using the improved EDD algorithm based on the danger theory. The proposed method uses NS-2 to carry out simulation experiments. In this experiment, the network consists of 50 mobile nodes and replica nodes, the number of replicas

changes over time. The simulation parameters used in this technique are shown in Table 1, and these parameters are used to construct the network.

Table 1 Simulation Parameters

Simulation Parameter	Value
Propagation mode	Two ray ground
Channel	Wireless channel
Physical layer	Wireless physical layer
Queue	DropTail/Priority queue
MAC protocol	802.11
X dimension	500
Y dimension	500
Routing protocol	AODV
Antenna	Omni antenna
Number of packets	100
Simulation nodes	10~60
Simulation time	200~10000s
AODV Min neighbor	6
AODV Security time	4
Number of replicas	5~25

5.1. Evaluation Index

The performance of this work is analyzed using the routing overhead, packet delivery ratio, energy consumption, positioning error and the average packet delay and other indicators. The detection rate is used to measure the accuracy of replica node detection. Figure 3~6 shows the performance of the algorithm in terms of energy consumption, packet delivery ratio, average delay and detection rate.

Energy consumption is a percentage of energy consumption, can be calculated by the formula (10).

$$\text{Average energy consumptio n} = \frac{\text{Sum of energy consumptio n of all nodes}}{\text{Number of nodes}} \quad (10)$$

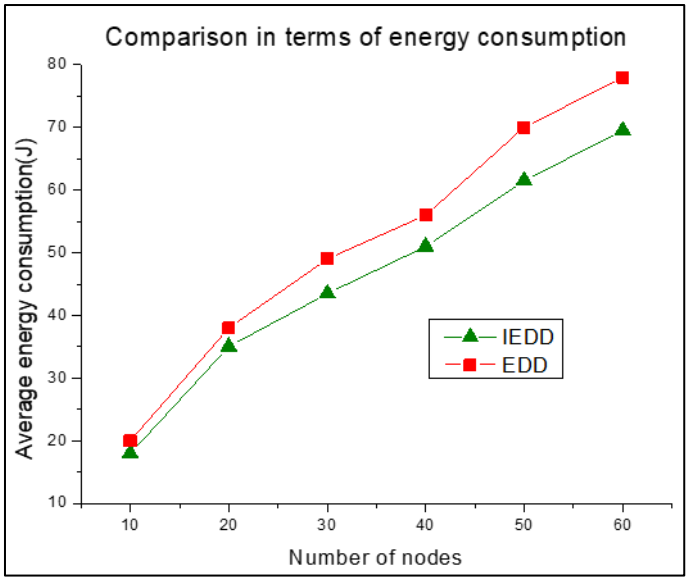

Figure 3 Comparison Between IEDD and EDD in Terms of Energy Consumption

Figure 3 is the energy consumption graph, which shows that the proposed IEDD algorithm has lower energy consumption. The energy consumed is expressed as joule.

Packet delivery ratio is the ratio of the number of packets received at the receiving end to the total number of packets sent by the sender, see formula (11).

$$\text{Packet delivery ratio} = \frac{\text{Number of successful ly received packets}}{\text{Total number of packets sent}} \quad (11)$$

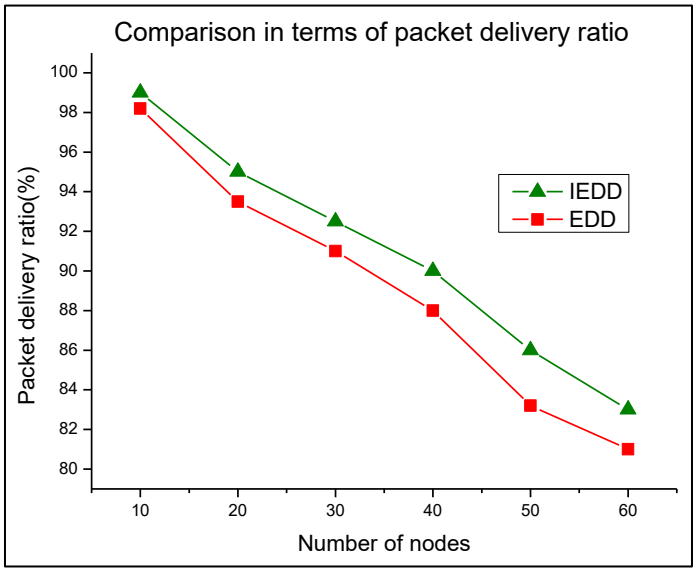

Figure 4 Comparison Between IEDD and EDD in Terms of Packet Delivery Ratio

Figure 4 shows the packet delivery ratio, which indicates that the proposed IEDD algorithm has a higher packet delivery ratio than the EDD algorithm. Packet delivery ratio is expressed as a percentage.

Average delay is the average of all the received packets' time delay; it is calculated by the formula (12).

$$\text{Average delay} = \frac{\text{Delay of all packets}}{\text{Total number of received packets}} \quad (12)$$

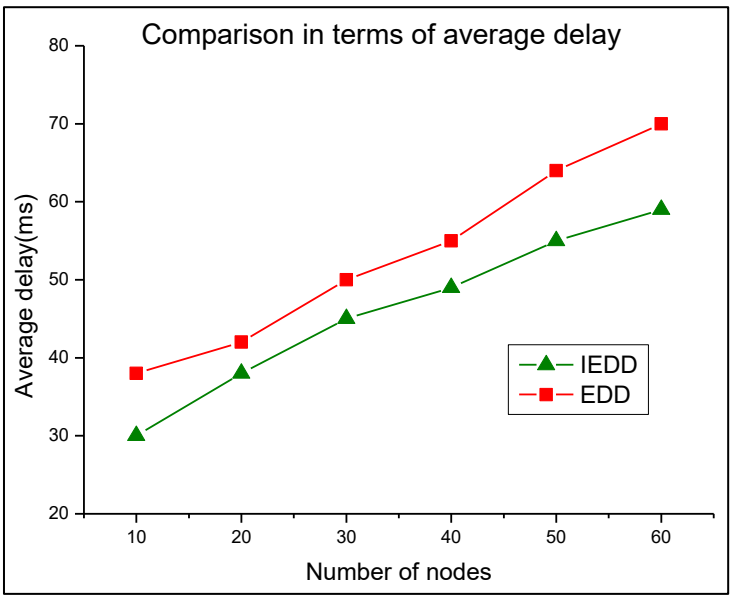

Figure 5 Comparison Between IEDD and EDD in Terms of Average Delay

Figure 5 shows the average packet delay; it can be seen that the average delay of the proposed IEDD algorithm is lower than the EDD algorithm. Average delay is expressed as seconds.

The detection rate is the proportion of successfully detected replicas accounted for total number of replicas, and is expressed as a percentage.

$$\text{Detection rate} = \frac{\text{Successful ly detected replicas}}{\text{Total number of replicas}} \times 100\% \quad (13)$$

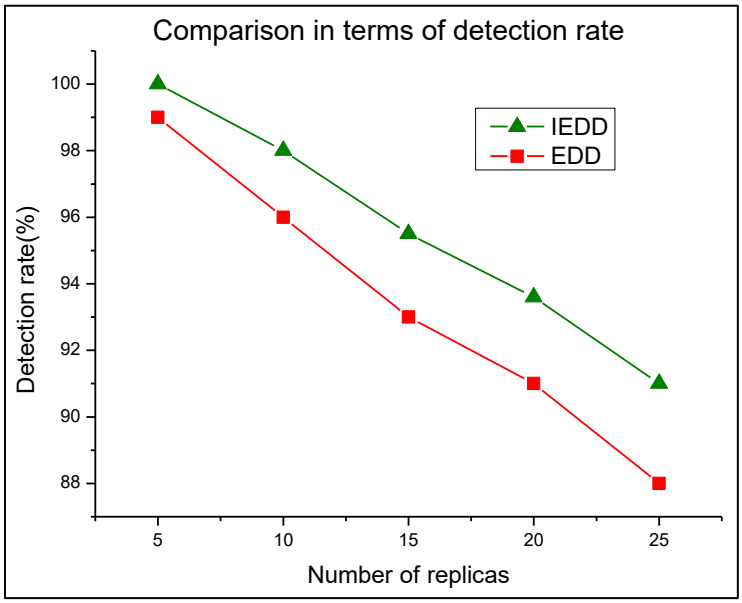

Figure 6 Comparison Between IEDD and EDD in Terms of Detection Rate

Figure 6 shows the detection rate; we can see that the IEDD algorithm has a higher detection rate than the EDD algorithm.

6. Conclusion

Security is the most important problem in wireless sensor networks. The degradation of network performance can be caused when there are multiple replicas in the network. This paper mainly focuses on the detection of node replication attacks. A variety of replica detection methods have been used to deal with node replication attacks. The danger theory based IEDD algorithm has the characteristics of low energy consumption and low false alarm rate, which is very suitable for wireless sensor networks. The comparison of the proposed IEDD algorithm and the existing EDD algorithm was carried out by experiments. The results show that the average delay, energy consumption, system overhead and packet loss rate have been decreased, and the packet delivery ratio and detection rate have been improved.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Geetha C , Ramakrishnan M .Replica Node Attack Detection Approaches in Static WSNs[J].Advances in computational sciences and technology, 2023, 16(2):141-150.

[2] Sujihelen L, Boddu R, Murugaveni S, et al. Node replication attack detection in distributed wireless sensor networks[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 7252791.

[3] Sajitha M, Kavitha D, Reddy P C. An optimized whale based replication node prediction in wireless sensor network[J]. Wireless Networks, 2022, 28(4): 1587-1603.

[4] Alrashed E A, Karaata M H, Hamdan A A. Malicious replica quarantining protocol for Mobile Wireless Sensor Networks using replica detection and identification[J]. Internet of Things, 2024, 27: 101289.

[5] Yu, C. M., Tsou, Y. T., Lu, C. S., & Kuo, S. Y. (2013). Localized algorithms for detection of node replication attacks in mobile sensor networks. IEEE Transactions on Information Forensics & Security, 8(5), 754-768.

[6] Anitha S, Jayanthi P, Chandrasekaran V. An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks[J]. Measurement, 2021, 167: 108272.

[7] Jacob S S, Karthikeyan B, Johnpeter T, et al. Deployment with location knowledge by multi area approach for detecting replica nodes in wireless sensor network[J]. Tehnicki Vjesnik-Technical Gazette, 2024, 31(1): 254-261.

[8] Sujihelen L, Senthilsingh C. Detect the replica node in mobile wireless sensor networks[C]//2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2021: 265-267.