Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3321870, 9 pages
https://doi.org/10.1155/2022/3321870

Research Article

Enhanced Lion Optimization with Efficient Path Routing Equalization Technique against DoS Attack in Wireless Sensor Network

R. Elavarasan,[1] **K. Chitra**,[2] **and Amsalu Gosu Adigo**[3]

[1]*Faculty of Electronics Engineering Sathyabama University, India*
[2]*School of Electronics Engineering, VIT University, Chennai, 600119 Tamil Nadu, India*
[3]*Center of Excellence for Bioprocess and Biotechnology, Department of Chemical Engineering, College of Biological and Chemical Engineering, Addis Ababa Science and Technology University, Ethiopia*

Correspondence should be addressed to R. Elavarasan; elavarasanphd1@gmail.com
and Amsalu Gosu Adigo; amsalu.gosu@aastu.edu.et

Received 2 March 2022; Revised 28 April 2022; Accepted 29 April 2022; Published 14 June 2022

Academic Editor: Mohammad Farukh Hashmi

In WSN, DoS (denial of service) attack makes shortcoming system. The packets travel over and over in the sensor network. By that, all the assets like data transmission, memory, and vitality are squandered by this attack. However, the attacker ought to optimize its attacker plan for request to boost the impact on the system performance because of the deficiency of vitality at the aggressor side. Denial of service (DoS) attack on the Internet has become a squeezing issue. By staying away from these sorts of attacks, network performance can be improved. Therefore, security is a fundamental requirement for these networks. Effective routing is necessary in order to overcome the issued faced by the crosslayer in the DOS attack of the WSN network for the purpose of good transmission. This research work mainly focuses on performance evaluation using optimization methods. To establish the efficient path in the crosslayer against DoS attack, this paper has proposed enhanced lion optimization with an efficient path routing equalization technique (LOEPRE). If any failure node occurs in the network, then the node is recognized and the transfer of the data packet is done to the other node. Retransmission of data causes overload in the network. The proposed model focuses on these issues and overcomes these issues by improving the path efficiently with robust security. It consists of three phases: the initial phase includes the route discovery in the network. In the second phase, the transfer of data is done in the high router path for security purposes. Finally, the efficient path routing equalization technique is used for minimizing the overload in the network; it provides the equalized path length in the network and is highly efficient. Hence, the proposed LOEPRE technique is used to achieve energy efficiency in wireless network for prolonged network lifetime and minimum packet latency and minimize consumption of energy. Moreover, the simulation outcome of the proposed LOEPRE method is highly robust while comparing to the existing methods EFCRS, SSPRA ELOER, EFLOR, and TSTP. It achieves better performance than existing algorithms in comparing metric connectivity ratio, end-to-end delay, overhead, throughput, and packet delivery ratio.

1. Introduction

The principal attributes of a WSN include the following: WSNs are getting a great deal of enthusiasm by the researchers and industry because of their less cost solutions for different real-world issue solving applications. The main advantage of this is the less vitality, heterogeneity, and mobility on the usage of hubs. It can survive amidst bad conditions, and the adaptation of the sensor is better.

In WSN, threats are from outside the system and inside the system. In the event that attacks are from the hubs of the local system, then it is much harmful. Likewise, it is very hard to discover the malicious or compromising node inside

the local system. The attacks of WSN can be arranged into two categories: intrusive and nonintrusive. Nonobtrusive assaults for the most part focus on timings, power, and recurrence of the channel. Intrusive assaults focus on the accessibility of administration, transit of data, routing, and so on. In DoS attacks, the hacker tries to make the service or framework difficult to reach. Anyway, during the transit of data, progressively normal assaults are experienced. Path-based DoS are a sort of attack where a number of hubs which are available in the path from source to the base station towards the sending data are depleted by the quantity of fake parcels, sent to the way towards base station. Under such conditions, the hub gets occupied and it denies for real traffic transmission.

The design of crosslayer is one of the enormous areas in networking research. The cooperation in crosslayer implies empowering the transmission of layers with one among the perhaps noncontiguous layers in the convention stack. Generally, the conventions of system are ordered into various free layers. Each layer is formulated separately, and the correspondence in the middle of those layers is executed through a very much characterized interface. One of the principal advantages of utilizing this is structural strength. The term crosslayer names the consumption of energy, mobility, bad performances, wireless routes, consumption of energy, quality of service, loss of packets, and complications of delay that are noticed in the wireless sensor networks.

If any failure node occurs in the network, then the sender can retransmit the data packets again. Retransmission of data causes overload in the network. The proposed model focuses on these issues and overcome these issues by improving the path efficiently with robust security. To establish the efficient path in the crosslayer, this paper has proposed enhanced lion optimization with efficient path routing equalization technique (LOEPRE). This technique is used to establish a route to transfer data with high security level and minimize the overload in the network; it also provides the equalized path length in the network and is highly efficient.The main aim of the proposed LOEPRE method is, the less energy consumption, increasing life span, less data latency in the WSN network. The objective is to establish the efficient and secure path for the transmission of data in crosslayer to avoid DoS attack in WSN.

This paper is organized as follows. Section 2 presents a brief literature review including optimization techniques and how to avoid DoS attacks in WSN. Section 3 presents the problem definition. Section 4 presents the proposed work, algorithm used, and process flow. Section 5 presents the performance analysis and simulation result discussion, Finally, Section 6 provides the conclusion of the proposed work.

2. Literature Review

Cao et al. [1] has created AccFlow which is a steadily deployable software-defined networking-based convention that can fill in as a countermeasure against the low-rate TCP DoS attack. The principle thought of AccFlow is to make the attack flows responsible for the blockage by dropping their parcels as per their loss rates. The bigger their loss rates, the more aggressively AccFlow drops their parcels. Through broad reenactments, they show that AccFlow can successfully shield against the low-rate TCP DoS attack regardless of whether aggressors change their techniques by assaulting at various scales and information rates. Besides, while AccFlow is intended to explain the low-rate TCP DoS assault, they exhibit that AccFlow can likewise successfully shield against general DoS assaults which do not depend on the TCP retransmission break instrument yet motivation denial of service to authentic clients by reliably debilitating the system assets. Lastly, they consider the adaptability of AccFlow and its arrangement in genuine systems.

Kanagasabapathy et al. [2] proposed two approaches in the cluster-based sensor system to identify the maliciousness level of hubs to verify sensor systems from jamming assaults. The first methodology recognizes maliciousness level of hubs utilizing two modules, in particular, affirmation module and checking module. The accreditation module safeguards the system from the jammers. The checking module finds the sensor hubs that are stuck by a jammer. The second methodology utilizes fluffy rationale for improving the sticking measurements to decide the event of sticking precisely. The proposed framework accomplishes 99.58% location proportion to decide hub's maliciousness level.

Aborujilah et al. [3] have presented effective methods for gathering, preparing, and distributing information. Wireless sensor networks assume an essential job in the extending development of internet of things (IoT). In any case, DoS assaults are a significant risk of WSNs. Right now, a hypothesis-based model has been proposed to dissect the security of WSN under DoS assaults. The proposed model portrays and evaluates the security of WSN when it experiences DoS assaults by finding the assault achievement likelihood, assault cost, assault impact, mean time-to-compromise, assault hazard, and profit for assault esteems. The effect of alleviation techniques towards reinforcing the WSN security has been portrayed. Brilliant home scenario WSN has been attached for instance. The outcomes demonstrated the capacity of the proposed model to investigate the impacts of DoS assaults in WSN. Additionally, it indicated the effect of mitigation techniques in improving WSN security.

Krishnan [4] has investigated that wireless sensor networks (WSN) have incredible advantages of diminished costs and lesser adaptability factor and can be utilized upon complex and hazardous areas with the end goal of control/robotization of assignments and for detecting, preparing, and sharing/sending information. Denials of service (DoS) assaults frustrate the ordinary working of such systems prompting compromise of the goals of them. Hence, work which has a progressive hierarchical clustering approach is proposed to distinguish the trade-off of hubs in WSN because of DoS assaults. This methodology exceeds different methodologies in the part of end of outliers and quicker reaction time in detecting the attacks.

In Hafizullah et al.'s study [5], low-force and high-performance WSNs permit adaptable demonstrating of IoT. MANETs transcendently convey ad hoc on-demand distance vector (AODV) steering technique to create routes responsively. AODV sends the destination arrangement number by

which it gives circle free courses. In this paper, equipment engineering for the usefulness of the route discovery process used in AODV routing convention is demonstrated and actualized utilizing Verilog equipment depiction language and integrated in XC4VLX25 device. In addition, some parameter constants have likewise been contemplated to actualize a route discovery mechanism for the continuous situation.

Iyer et al. [6] have investigated that multilevel picture segmentation is a basic undertaking in picture handling that includes various limit esteems. As the high computational expense of a comprehensive inquiry is wasteful and lumbering, the ideal edge calculations make for a superior way to wander; subsequently, an analysis of advancement calculations to set the ideal edges is profoundly basic and useful. This paper presents that practical comparison is made to conclude the best enhancement method among the whale streamlining and antlion advancement calculation, to take care of the staggered limit issue, and to locate the optimal multilevel thresholds. Otsu's function is augmented to perform upgraded thresholding-based picture segmentation. The test results indicated that the antlion enhancement calculation gave better execution in tackling the issue for more significant level multithresholding.

Goyal and Sharma [7] have investigated that WSN sink hub assumes a noteworthy role in the handling of information. In the various categories of WSN, two assortments of sink hub are used, for example, static sink hub and mobile sink hub. This exploration paper for the most part is centered around the exhibition assessment of portable sink hub utilizing metaheuristic enhancement methods, for example, insect settlement streamlining, antlion optimization, gray wolf enhancement, and cuckoo search based on following quality of service parameter total packet received, total packet dropped, packet delivery ratio, throughput, average end-to-end delay, and energy consumed. Reenactment results and analysis of information investigated that GWO gives better outcomes as contrast with different systems.

In a mobile sensor network with a mobile sink, picking the next hop relies upon the present area of the sink. This requires a frequent update of directing ways inside the system. In Nuruzzaman and Ferng's study [8], route quality indicator (LQI) estimated by a sensor while getting a POLLING packet legitimately from the sink is utilized to obtain the general situation of the sensor to the sink. Thusly, the sensor picks the next hop with a higher LQI esteem. Because of the heterogeneity of transmission power and for ensuring the reachability of the picked next hop, an energy-effective and reliable LQI-based beaconless steering (LQI-BLR) convention is proposed. To abstain from flooding REPOLLING parcels, just the sensors with low LQI values are permitted to communicate the REPOLLING packet to make a directing way for the sensors outside the transmission range of the sink.

In the survey, the last two perspectives have not got a lot of consideration compared with the exactness of WSN time synchronization. Particularly in multihop WSNs, middle gateway hubs are overburdened with undertakings for handing-off messages as well as an assortment of calculations for their overloaded hubs just as themselves. In this manner, limiting the vitality utilization as well as bringing down the computational unpredictability while keeping up the synchronization exactness is significant to the plan of time synchronization plans for resource-constrained sensor hubs.

In Huan et al.'s study [9], focusing on the three parts of WSN time synchronization, they present a system of reverse asymmetric time synchronization for resource-constrained multihop WSNs and propose a beaconless energy-efficient time synchronization plot dependent on inverted one-way message dissemination. Exploratory outcomes with a WSN testbed dependent on TelosB bits running TinyOS show that the proposed plan moderates up to 95% vitality utilization compared with the flooding time synchronization convention while accomplishing microsecond-level synchronization exactness.

In Premanand and Rajaram's study [10], as we know, the network that has the mobile nodes sometimes is unstable that may also does not maintain the accuracy of data. In order to rectify the proposed method called enhanced data accuracy-based path discovery, it is introduced to receive the data in which accuracy rate is so high. Further, it can detect congestion; energy consumption and size are reduced.

Rajaram and Palaniswami [11]. Here we have introduced a security system that is a trust based protocol depend on the Mac layer method which reaches the confidentiality and authentication of packets. It has packets in routing layer and MANET that have link layer. The delivery percentage of packets is increased when a low delay occurs, speed is high.

From Rajaram and Palaniswami's study [11], here, we initiated to create an enhanced distributed certificate authority scheme in the motive to give away the data of high integrity. While doing so, the network we use becomes more secure inwards and also outwards. The results show more packet delivery when low delay and overhead occur.

3. Problem Definition

Identified with the routing protocol approach, it is vital to accept the security issues and energy plans offering criticalness to the quality of service. While performing the cluster-based routing procedure, various target capacities are considered to select the best possible cluster head with the expansion of the lifetime of the wireless sensor nodes. Fundamentally, the wireless sensor nodes contain a restricted measure of vitality to transmit the information. Thus, the system lifetime is the key characteristic utilized for surveying the performance of the wireless sensor network. Routers are intended to deal with enormous throughput that prompts the structure of high bandwidth; but issues occurred while establishing the route, issues like untrusted user, third party access, and path miscommunication. Therefore, the proposed optimization helps to outperform with better security and reliability.

Essentially, the lifetime of the sensor hubs is determined by the remarkable energy of the hubs. Therefore, the most significant challenge present in the WSN is utilized to build up the proficient utilization of energy resources in WSNs.

In [12], FABC technique is produced for routing, yet it creates another solution by moving the existing towards another solution by choosing a random solution from the populace. This seriously influences when the solution

arrived at a local optimum. From Figure 1, we can comprehend that the information transmission is performed through the group head to the sink hub. Here, the best possible choice of group head is one of the major testing undertakings present in wireless sensor network. So finding an optimized technique for the improvement of system lifetime, expanding the connectivity, recognizing the most limited routing procedure, focusing on the inclusion, and limiting the errors are essential. This is quite challenging, and it illustrates a wide open area for research in the field of outdoor wireless sensor networks.

4. Proposed Methodologies

The main aim of this proposed system is to establish the efficient and secure path for the transmission of data in crosslayer to avoid DoS attack in the wireless sensor networks. The major goal is to establish an efficient path for communication and to avoid the attacks faced by the wireless system. For analyzing its path, an algorithm called enhanced lion optimization with efficient path routing equalization technique is developed. This algorithm is mainly used to avoid DoS attack in crosslayer and creates an efficient path for data transmission with security. This method helps in selecting the efficient path for routing with less energy consumption. The contribution of this proposed work is as follows:

(i) To establish crosslayer route for data transmission and to balance the overload in system

(ii) After creating the crosslayer route, the node is analyzed

(iii) Enhanced LOEPRE technique is proposed to avoid DoS attack in the crosslayer and establish an efficient path for node communication and routing purpose

(iv) Efficient path equalization routing technique is presented for flexibility, and the efficient path for each sensor node is optimized

(v) Enhanced LOEPRE technique performance is predicted with the support of NS2 simulation

Figure 2 describes the overall procedure of the proposed enhanced LOEPRE technique. Initially crosslayer route is established, and if any fault occurs while transmitting, then the retransmission process is applied so overload can occur. To overcome the packet loss and avoid DoS attack and efficient path transmission, the enhanced LOEPRE technique is proposed to create efficient path in crosslayer against DoS attack. This proposed LOEPRE technique is used for controlling overload, minimizes packet delay and network efficiency, has reliable data transmission, and also creates an efficient path in cross layer.

4.1. Route Establishment in Crosslayer. In this section, crosslayer interface is built up in wireless sensor systems. The crosslayer configuration ought to be in the structure that joins data and reasons for both crosslayer and traditional transmission layers in the single convention. In providing the structure of crosslayer connections, there exist a number of preferences. This incorporates interoperability, congestion control, and improved plan of transmission conventions. By establishing the crosslayer in the system, it permits each hub to decide on including in transmission. Subsequently an entirely distributed and flexible operation is utilized. Initially, the sensor hub begins the correspondence by sending the bundle RTS (Request to Send) packets to show the close by hub that it has packets to transmit. Hence, the performance of the crosslayer design determines the sensor node to involve communication. With these constraints, crosslayer design satisfies the handling of local congestion, hop-by-hop trustworthiness, and distributed performance. Once the route is established, then the procedure of LOEPRE begins.

4.2. Enhanced Lion Optimization Technique. This proposed enhanced lion optimization technique is used to generate the energy efficient routing protocol in wireless sensor network. This technique is based on the behavior and social organization. It is used to find and replace the worst path by the best path. This algorithm is mainly used to monitor the behavior of the sensor node found in the routing path. This technique is strong local search and assists enhanced lion optimization (ELO) to search around a path to improve it. This moves towards the selected area in random numbers with uniform distribution. The distance between the intermediate nodes and sensor node position is selected to illustrate the original direction for transmission. If there are any attackers, then this technique is used to select another path with high security for communication. Routers are relied upon to provide the best effort packet forwarding, while the sender and the receiver are liable for achieving desired service guarantees, for example, quality of service and security. Routers are intended to deal with enormous throughput that prompts the structure of high-bandwidth pathways in the intermediate network. This attack mainly occurs due to less bandwidth of end-host than routers. If a DoS attack has occurred in the crosslayer, the proposed LOEPRE technique is implemented to avoid this attack with an efficient path and higher security for a robust network.

After establishing the route in the crosslayer network, the sensor network node is selected with trustworthiness of node and it performed frequency transmission in Algorithm 1. If the sensor node is equal to anomaly, the communication is obstructing. This may get overhead, but the sensor node is not equal to the anomaly; the communication is performed effectively. Therefore, the network lifetime is improved with reduced delay.

4.3. Efficient Path Equalization Routing Technique. This proposed technique is used effectively to reduce the energy consumption and shorten the transversal path. The path length of nodes in the network is distributed and optimized to maximize the lowest probability of the energy consumption of the entire network. Since the characteristics of nodes may vary often, so, this algorithm finds the suitable node for communication in an efficient way. This selects routing

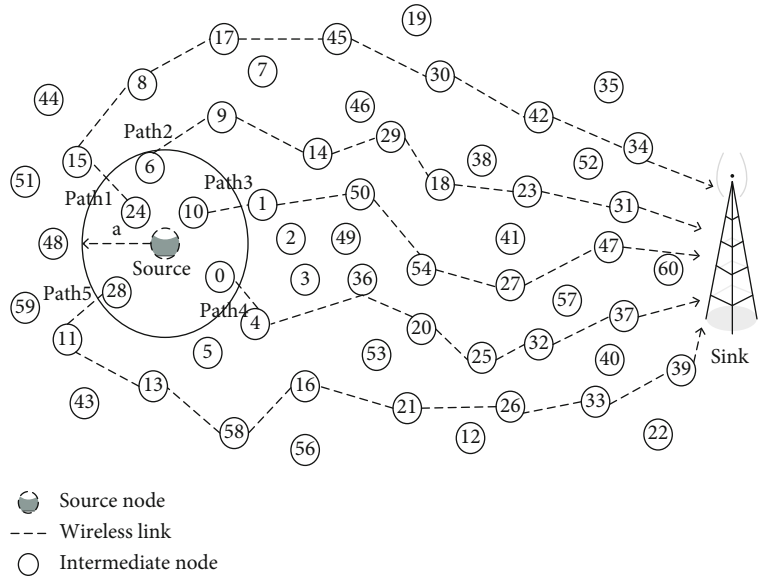

Figure 1: Wireless sensor network model.

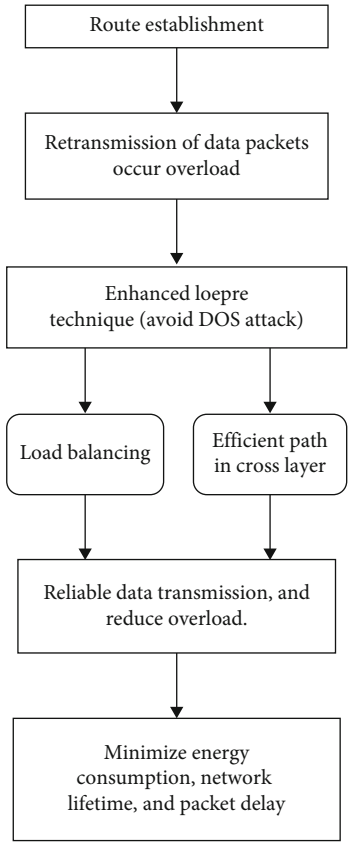

Figure 2: Block diagram of enhanced LOEPRE.

nodes from starting to end nodes with lesser energy consumption. This work plans the multipath nodes in the case of data collections, to achieve the shortest path in the efficient way. The node arrangements are transported in the random way. Efficient path equalization routing technique

Step 1: establish route in crosslayer network
Step 2: find the node in network is trustworthy
Step 3: frequent transmission
Step 4: if node==anomaly
Step 5: communication is obstructed
Step 6: overload occurred
Step 7: else
Step 8: if node! = anomaly
Step 9: communication can be performed
Step 10: improves network lifetime and reduce delay
Step 11: end
Step 12: end process

Algorithm 1:

is presented for flexibility, and the efficient path for each sensor node is optimized. This proposed technique is mainly used for path efficiency and to provide an efficient path against DoS attack in the crosslayer.

In Algorithm 2, in the proposed LOEPRE scheme, the efficient path is selected for the sensor node to communicate. It has less energy utilization and has high security compared to the existing (EFCRS, SSPRA ELOER, EFLOR, and TSTP) techniques. It acquires high throughput in the destination node. Introducing an efficient path equalization routing with an enhanced lion optimization technique minimizes the overload; it finds the efficient path for communication in crosslayer, minimizes congestion in the network, and also provides an efficient path in the crosslayer against DoS attack.

4.4. Proposed Packet Format. Packet ID: this packet contains the features of sensor nodes in the network. It consists of the sensor nodes and their behavior.

Step 1: path discovery in crosslayer network
Step 2: efficient routing path against DoS attack
Step 3: search efficient routing path for node communication
Step 4: if node = =reliable
Step 5: transmission proceeds on the same path
Step 6: else
Step 7: if node! = reliable
Step 8: discover suitable efficient routing path
Step 9: energy consumption, improves path balance, and flexibility.
Step 10: end

Algorithm 2:

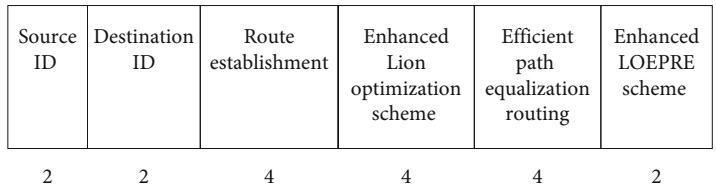

Figure 3: Proposed packet format.

The packet format of the proposed LOEPRE scheme is given in Figure 3. The first and second field comprises of node's source ID and destination ID. Each field occupies 2 bytes. The third field is the establishment of route in the crosslayer; this field occupies 4 bytes. The fourth field is for the status of nodes behavior with security. The behaviors of nodes are analyzed based on its ELO, and this field occupies 4 bytes. The fifth field is for efficient path equalization routing. This is for finding the efficient path for nodes to communicate in the network. This algorithm helps in finding the efficient path in the crosslayer against DoS attacks. This field occupies 4 bytes. The last field is for the enhanced LOEPRE scheme. This establishes the efficient path based on the node's energy. This field occupies 2 bytes.

4.5. Simulation Result. In order to simulate the proposed method LOEPRE, Network Simulator NS-2.34 version is utilized. Network Simulator is a discrete event simulator, and it offers impressive guide of simulation of routing, multicast protocols, and TCP for the two wired and furthermore wireless networks. NS-2.34 satisfies adequate protocol plans, and coding can be reached in the absence of any unpredictability.

In our proposed method simulation, around 100 sensor nodes go in the region of a 1100 meter × 950 meter square region with simulation time of 50 milliseconds. Mac address 802.11 g is assimilated with design, and all the nodes acquire fixed range of coverage of around 250 meters. Major protocol uses DSDV. Each packet size is 512 bytes with random way point of mobility model. The setup of simulation and its parameters are defined in Table 1.

Table 1: Simulation setup of the proposed protocol.

No. of nodes	100
Area size	1100 × 950
Mac	802.11 g
Radio range	250 m
Simulation time	50 ms
Traffic source	CBR
Packet size	512 bytes
Mobility model	Random way point
Protocol	DSDV

5. Performance Analysis

In simulation, performance metrics using X graph in ns2.34 are analyzed.

5.1. Energy Consumption. Figure 3 presents the consumption of energy. It is the complete energy which is employed for specific data communication; choose from its initial level to the endmost energy level. In the proposed LOEPRE scheme, it illustrates the reduced energy consumption when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP. Energy consumption is obtained for 1000000 node level.

$$\text{Energy consumption} = \text{initial energy} - \text{final energy}. \quad (1)$$

5.2. Communication Overhead. Figure 4 illustrates the comparison rate of overhead during transmission in network that arises at the duration of broadcasting data packets for whole communication from the sender node to the sink

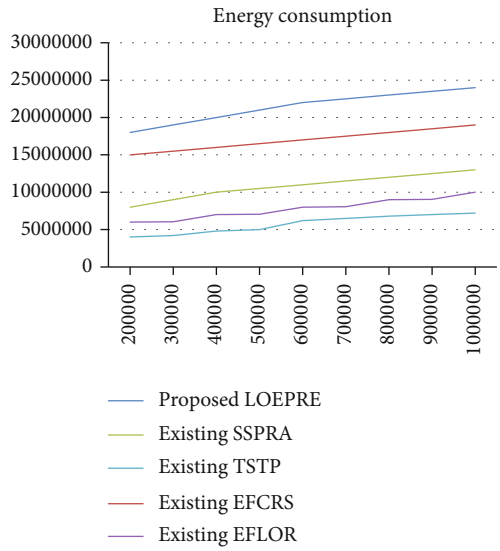

Figure 4: Graph for number of nodes vs. energy consumption (%).

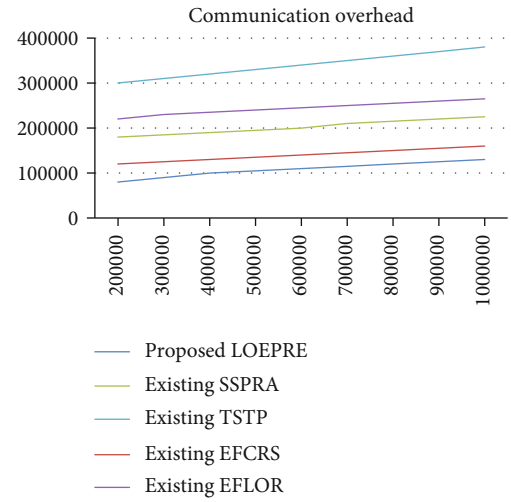

Figure 5: Graph for number of nodes vs. communication overhead (%).

node. Network overhead is obtained for 1000000 node level. Minimum overhead is achieved for the proposed LOEPRE with 100000 levels. In the proposed LOEPRE scheme, overhead in the communication is less when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

$$\text{Communication overhead} = \left(\frac{\text{number of packet losses}}{\text{received}}\right) * 100. \quad (2)$$

5.3. End-to-End Delay. Figure 5 illustrates the comparison rate of end-to-end delay which is analyzed by estimating the time occupied for communication of packets from a sender node to the destination node; every sensor node is created with the support of an IP address. In the proposed LOEPRE scheme, end-to-end delay is minimized when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

$$\text{End-to-end delay} = \text{end time} - \text{start time}. \quad (3)$$

5.4. Detection Efficiency. Figure 6 illustrates that detection efficiency is the estimated amount of time taken to detect the misroute packet along with the network; ELO technique forwards data in multiple flow manners to various paths. In the proposed ELO method, detection efficiency is increased and distinguished from previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

$$\text{Detection efficiency} = \frac{\text{attack detection rate}}{\text{overall time}}. \quad (4)$$

5.5. Link Stability. Figure 7 illustrates the comparison graph for link stability. This rates the stability of the network. From the graph, it is seen that the proposed LOEPRE scheme attains

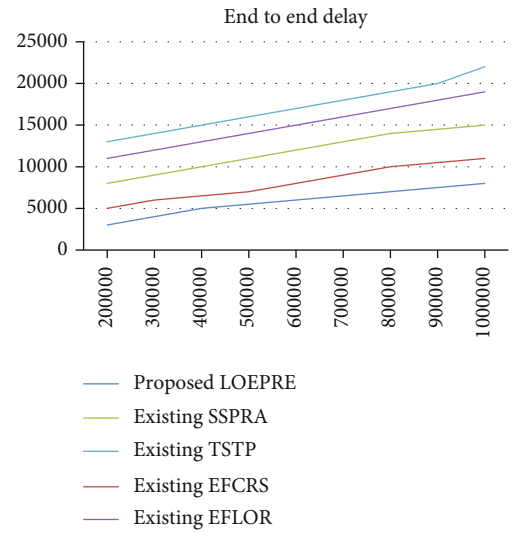

Figure 6: Graph for mobility (sec) vs. end-to-end delay (sec).

high link stability when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

5.6. Throughput. Figure 8 illustrates the comparison of throughput. It is measured as the quantity of data that transfers successfully from the intermediate node to the sensor node in the specific provided time. In the proposed LOEPRE scheme, throughput is improved when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

$$\text{Throughput} = \left(\frac{\text{number of packet received}}{\text{sent}}\right) * \text{speed}. \quad (5)$$

5.7. Packet Delivery Ratio. Figure 9 illustrates the comparison of packet delivery ratio that is analyzed by a measure of attainable packets from a number of transmitted packets in specific speed. In the proposed LOEPRE method, packet delivery ratio

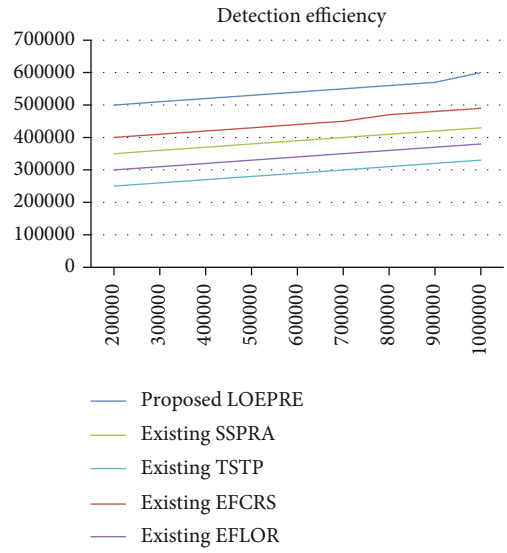

Figure 7: Graph for nodes vs. detection efficiency.

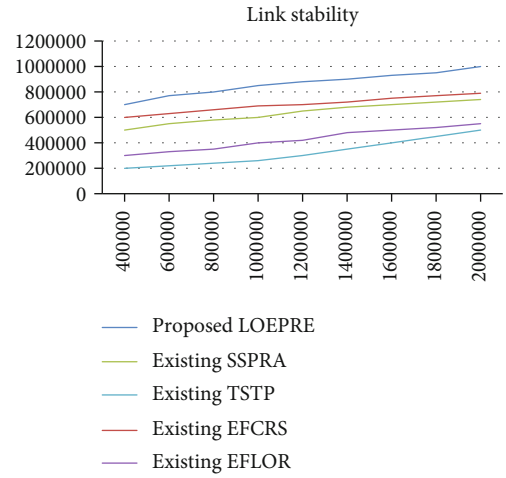

Figure 8: Graph for speed (ms) vs. link stability (%).

is improved when compared to other previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

$$\text{Packet delivery ratio} = \left(\frac{\text{number of packet received}}{\text{sent}}\right) * \text{speed}. \tag{6}$$

5.8. Network Lifetime. Figure 10 demonstrates that lifetime of the network is estimated by node process time taken to use arranged from overall system capacity; it has congestion control convention strategy to give overload free communication path; it discovers and keeps away from blockage node accessible in the route. In the proposed LOEPRE method, network lifetime is improved compared with previous strategies EFCRS, SSPRA ELOER, EFLOR, and TSTP.

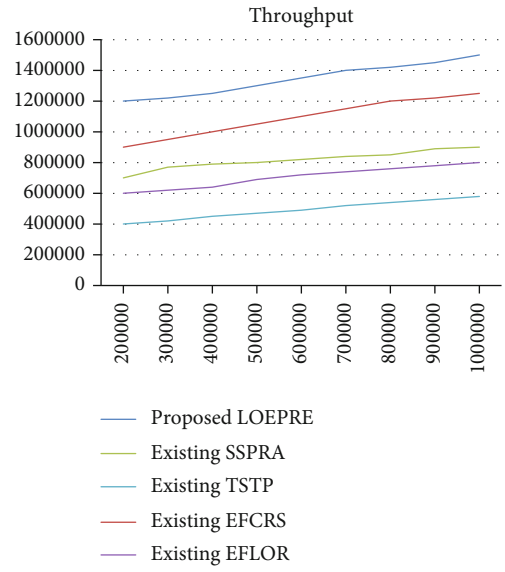

Figure 9: Graph for number of nodes vs. throughput (mbps).

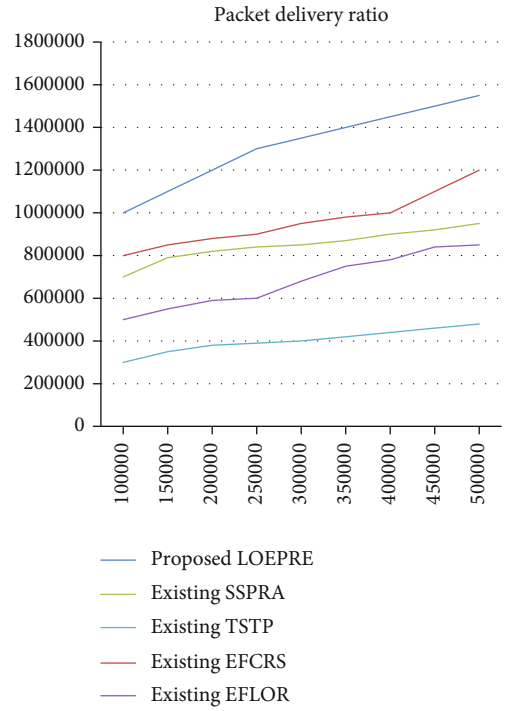

Figure 10: Graph for mobility (bps) vs. packet delivery ratio (%).

$$\text{Network lifetime} = \frac{\text{time taken to utilize the network}}{\text{overall ability}}. \tag{7}$$

In Figure 11, the performance of energy, end-to-end delay, overhead, throughput, detection efficiency, link stability, packet delivery ratio, and network lifetime obtains the results and it achieves the improved performance result than existing works.

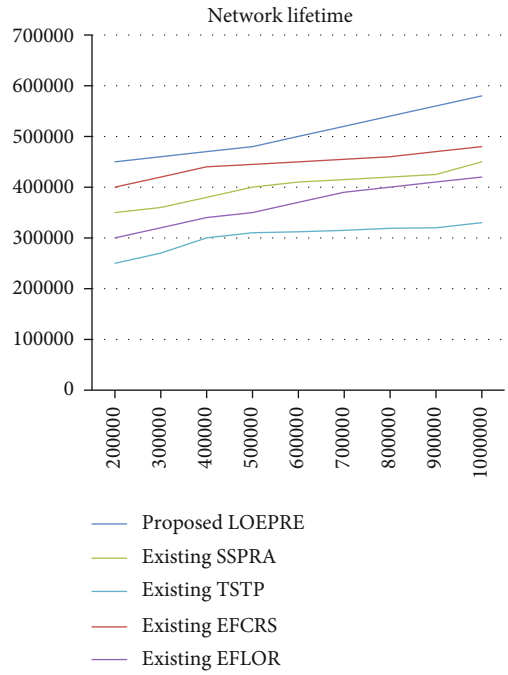

Figure 11: Graph for nodes vs. network lifetime (%).

6. Conclusion

Enhanced lion optimization with efficient path routing equalization (LOEPRE) technique is proposed, to avoid DoS attack from crosslayer and to create an efficient path to transmit data packets. This technique is used to establish a route to transfer data with high security level and minimize the overload in the network; it also provides the equalized path length in the network and is highly efficient. This technique is also used to reject the failure node in the crosslayer and create an efficient path for communication against DoS attack with higher security. Hence, the proposed LOEPRE technique is used to achieve energy efficiency in wireless network for prolonged network lifetime and minimum packet latency, reduces consumption of energy, and achieves network lifetime. The simulation outcome of the proposed LOEPRE method is highly robust while comparing to the existing methods EFCRS, SSPRA ELOER, EFLOR, and TSTP. It achieves better performance than existing algorithms in comparing metric connectivity ratio, end-to-end delay, overhead, network lifetime, throughput, and packet delivery ratio. In future work, the optimization with swarm intelligence approach is performed to get improved results of WSN performances.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Disclosure

A preprint has previously been published [13].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. Cao, L. Han, X. Zhao, and X. Pan, "AccFlow: defending against the low-rate TCP DoS attack in wireless sensor networks," 2019, https://arxiv.org/abs/1903.06394.

[2] P. M. K. Kanagasabapathy, V. KedaluPoornachary, S. Murugan, A. Natesan, and V. Ponnusamy, "Rapid jamming detection approach based on fuzzy in WSN," *International Journal of Communication Systems*, vol. 35, article e4205, 2019.

[3] A. Aborujilah, R. M. Nassr, T. Al-Hadhrami et al., "Security assessment model to analysis DOS attacks in WSN," in *International Conference of Reliable Information and Communication Technology*, pp. 789–800, Cham, 2019.

[4] S. N. Krishnan, "Denial of service (DoS) detection in wireless sensor networks applying geometrically varying clusters," in *International Conference on Computer Networks and Communication Technologies*, pp. 1023–1030, Singapore, 2019.

[5] S. Hafizullah, S. Verma, M. Vaidya, and A. Naugarhiya, "An efficient hardware architecture for route discovery in AODV for a sensor node," in *2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*, pp. 70–74, Jaipur, India, 2019.

[6] S. Iyer, A. P. Nadkarni, and T. N. Padmini, "Antlion optimization and whale optimization algorithm for multilevel thresholding segmentation," in *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1, pp. 1–8, Vellore, India, 2019.

[7] H. Goyal and R. Sharma, "Performance evaluation of mobile sink using metaheuristic optimization techniques," in *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan*, Jaipur-India, 2019.

[8] M. T. Nuruzzaman and H. W. Ferng, "Design and evaluation of an LQI-based beaconless routing protocol for a heterogeneous MSN," *Wireless Networks*, vol. 26, pp. 699–721, 2019.

[9] X. Huan, K. S. Kim, S. Lee, E. G. Lim, and A. Marshall, "A beaconless asymmetric energy-efficient time synchronization scheme for resource-constrained multi-hop wireless sensor networks," *IEEE Transactions on Communications*, vol. 68, pp. 1716–1730, 2020.

[10] R. P. Premanand and A. Rajaram, "Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET," *Peer-to-Peer Networking and Applications*, vol. 13, pp. 2089–2098, 2020.

[11] A. Rajaram and S. Palaniswami, "Malicious node detection system for mobile ad hoc networks," *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 1, no. 2, pp. 77–85, 2010.

[12] R. Kumar and D. Kumar, "Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network," *Wireless Networks*, vol. 22, no. 5, pp. 1461–1474, 2016.

[13] R. Elavarasan and K. Chitra, "Enhanced LION optimization with efficient path routing equilization technique against DOS attack in WSN," 2021.