Enhanced LION Optimization with Efficient Path Routing Equilization Technique Against DOS Attack in WSN

[1]R. Elavarasan, [2]Dr. K. Chitra

[1]Research scholar, Faculty of Electronics Engineering Sathyabama University

[2]*Professor, School of Electronics Engineering, VIT University,*

Chennai - 600119, Tamilnadu, INDIA

elavarasan1304@gmail.com, me2007wp@gmail.com

ABSTRACT:

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. Hence, to overcome the issues faced by the cross layer in the presence of DOS attack in WSN. For reliable data transmission, effective routing is required. This research work mainly focuses on the performance evaluation using optimization methods. To establish the efficient path in the Cross layer against DOS attack, this paper has proposed Enhanced lion optimization with efficient path routing equalization technique (LOEPRE). If there is any failure node occurs in the network then the node is recognized and communication of data packets again transmitted in another node. 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. It consists of three phases: In initial phase include the route discovery in the network. In second phase, enhanced lion optimization technique is used for establish a route to transfer data with high security level. Finally, efficient path routing equalization technique is used for minimize the overload in the network, it provides the equalize path length in the network and is highly efficient. Hence, the proposed LOEPRE technique is used to achieve energy efficiency in wireless network for prolong network lifetime, minimum packet latency, minimize consumption of energy. Moreover, the simulation outcome of the proposed LOEPRE method highly robust while comparing to the existing methods EFCRS, SSPRA ELOER, EFLOR and TSTP. It achieves better performance than existing algorithms in comparing metrics connectivity ratio, end to end delay, overhead, throughput and packet delivery ratio.

KEYWORDS: Denial of service (DOS), lion optimization, efficient path routing equalization technique, route discovery, WSN, Load balance.

INTRODUCTION:

The principle attributes of a WSN include: WSN are getting a great deal of enthusiasm by the researchers, industry because of their less cost solutions for different real world issue solving applications. Other preferring variables of wireless sensor are low vitality utilization of hubs, versatility, unattended activity, capacity to withstand awful ecological conditions, having dynamic

system topology, to adapt to sensor hub malfunctioning and failures, Mobility of hubs, Heterogeneity of hubs, Topology and Deployment Scalability, Easy use.

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 non-intrusive. Non-obtrusive assaults for the most part focus to timings, power and recurrence of channel. Intrusive assaults focus to accessibility of administration, transit of data, routing and so on. In DoS attacks, hacker tries to make service or framework difficult to reach. Anyway during the transit of data, progressively normal assaults are experienced. Path Based Dos is a sort of attacks where 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 hub gets occupied and it denies for real traffic transmission.

The design of cross layer is one of the enormous areas in networking research. The cooperation in cross layer implies empower the transmission of layers with one among the perhaps non- contiguous 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 cross layer names the consumption of energy, mobility, bad performances, wireless routes, consumption of energy, Quality of Service, loss of packets, complications of delay that are noticed in the wireless sensor networks .

If there is 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 Cross layer, 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 equalize path length in the network and is highly efficient. . Hence, the proposed LOEPRE technique is used to achieve energy efficiency in wireless network for prolong network lifetime, minimum packet latency, reduces consumption of energy and achieves network lifetime.

In this section II presents a brief literature review including: optimization techniques and how to avoid DOS attacks in WSN. Section III problem definition, Section IV proposed work, section V performance analysis and simulations, Section VI conclusion of the proposed work.

LITERATURE REVIEW:

Cao, Y., Han, L.,et al., (2019) 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 don't 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, P. M. K., Kedalu Poornacharyet al., (2019) has two approaches are proposed in the cluster-based sensor system to identify the maliciousness level of hubs to verify sensor systems from jamming assaults. First methodology recognizes maliciousness level of hubs utilizing two modules, in particular, affirmation module and checking module. Accreditation module safeguards the system from the jammers. Checking module finds the sensor hubs that are stuck by a jammer. 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, A., Nassr, R. M.,et al.,(2019) has presents 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, 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 experience DoS assaults by finding the assaults achievement likelihood, assault cost, assault impact, mean-time-to-compromise, assault hazard and profit for assault esteems. The effect of alleviation techniques toward reinforcing the WSN security has been portrayed. Brilliant home scenario WSN has been attaching for instance. The outcomes demonstrated that the capacity of the proposed model to investigation the impacts of DoS assaults in WSN. Additionally it indicated the effect of mitigation techniques in improving WSN security.

Krishnan, S. N et al., (2019) has investigated that Wireless Sensor Networks (WSN) have incredible advantages of diminished costs, 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, sharing/sending information. Denials of service (DoS) assaults frustrate the ordinary working of such systems prompting compromise of the goals of them. Hence work 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.

Hafizullah, S., Verma, S., et al., (2019) Low force and high-performance WSN 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. 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, S., Nadkarni, A. P., et al., (2019) has investigated Multi-level 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 edges 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, 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, 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 multi-thresholding.

Goyal, H., & Sharma, R. Et al.,(2019) has investigated 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 center around the exhibition assessment of portable sink hub utilizing metaheuristic enhancement methods for example Insect settlement streamlining, Antlion Optimization, Gray wolf enhancement, Cuckoo search based on following quality of services parameters 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 an frequent update of directing ways inside the system. Nuruzzaman, M. T., & Ferng, H. W et al.,(2019), 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, a 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 haven't got a lot of consideration compared with the exactness of WSN time synchronization. Particularly in multi-hop WSNs, middle gateway hubs are over-burden 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. Huan, X., Kim, K. S., Lee, et al.,(2019) , focusing on the three parts of WSN time synchronization, they present a system of reverse asymmetric time synchronization for resource constrained multi-hop WSNs and propose a beaconless energy efficient time synchronization plot dependent on invert 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.

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 expanding 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 characteristics utilized for surveying the performance of the wireless sensor network.

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.

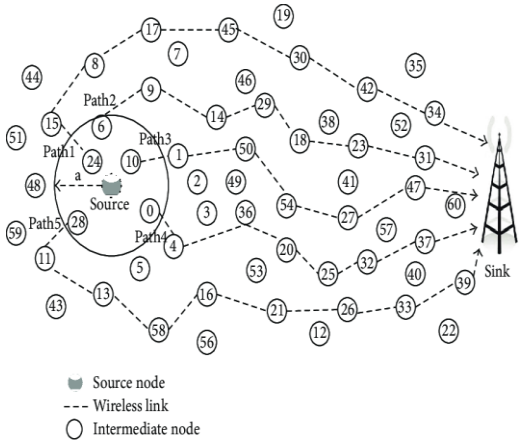


Figure 1: wireless sensor network model

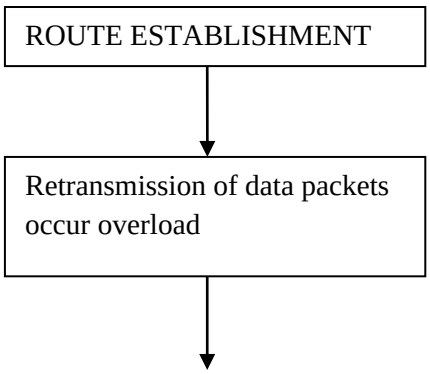
In [10], FABC technique is produced for routing yet it creates another solution by moving the existing towards another solution by choosing a random solution from the populace. This seriously influences when the solution arrived local optimum. From figure 1, we can comprehend the information transmission is performed through the group head to 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.

PROPOSED METHODOLOGIES:

The main aim of this proposed system is to establish the efficient and secure path for the transmission of data in cross layer to avoid DOS attack in the wireless sensor networks. The 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 cross layer 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 as follows:

- To establish cross layer route for data transmission and to balance the overload in system
- After creating the cross layer route, the node is analyzed.
- Enhanced LOEPRE technique is proposed to avoid DOS attack in the cross layer and establish an efficient path for node communication and routing purpose.
- Efficient Path equalization routing technique is presented for flexibility, and optimize the efficient path for each sensor node.
- Enhanced LOEPRE technique performance is predicted with the support of NS2 simulation.

Block diagram of proposed Enhanced LOEPRE scheme



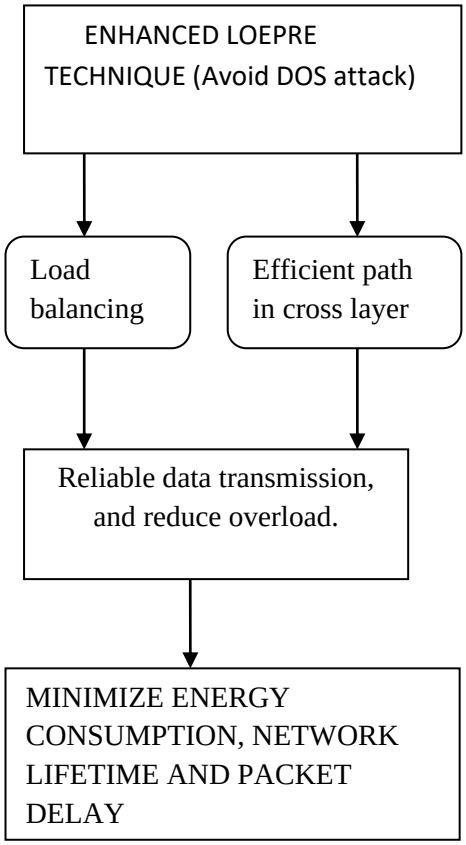


Figure 2: block diagram of enhanced LOEPRE

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

Route establishment in cross layer:

In this section cross layer interface is built up in wireless sensor systems. The cross layer configuration ought to be in the structure that joins data and reasons for both cross-layer and traditional transmission layers in the single convention. In providing the structure of cross-layer connects there exist a lot number of preferences. This incorporates interoperability, congestion control, and improved plan of transmission conventions. By establishing the cross-layer in the system, it permits each hub to decide on including in transmission. Subsequently an entirely distributed and flexible operation is utilized. Initially, 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 cross layer design which determines the sensor node to involve communication. With these constraints cross layer 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.

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 based on the behaviour and social organization. It is used to find and replace the worst path by the best path. This algorithm is mainly used to monitors the behaviour 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 nodes position are 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 DOS attack are occurred in the cross layer, the proposed LOEPRE technique is implemented to avoid this attack with efficient path and higher security for robust network.

Algorithm:

Step 1: establish route in cross layer network

Step 2: find the node in network is trustworthy.

Step 3: frequent transmission

Step 4: if node= =anomaly

Step 5: communication is obstruct

Step6: 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

Efficient path equalization routing technique:

This proposed technique is used effectively for reduce the energy consumption and shorten the transversal path. The path length of nodes in the network is distributed optimized to maximize the lowest probability of the energy consumption of the entire network. Since, the characteristics of node may vary often. So, this algorithm finds the suitable node for communication in efficient way. This selects routing nodes from starting to end node with lesser energy consumption. This work plans the multipath nodes in the case of data collections, to achieve the shortest path in efficient way. The node arrangements are transported in the random way. Efficient Path equalization routing technique is presented for flexibility, and optimize the efficient path for each sensor node. This proposed technique is mainly used for path efficiency and to provide an efficient path against DOS attack in the cross layer.

Algorithm:

Step 1: Path discovery in cross layer 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 proceed 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

Therefore due to this proposed LOEPRE scheme the efficient path is selected for sensor node to communicate. It consumes less energy utilization and high security comparing to the existing (EFCRS, SSPRA ELOER, EFLOR and TSTP) techniques. It acquires high throughput in the destination node. Due to introducing an efficient path equalization routing with enhanced lion optimization technique, it minimize the overload, it finds

the efficient path for communication in cross layer, minimize congestion in the network and also provide an efficient path in the cross layer against DOS attack.

Proposed Packet Format:

Packet ID: This packet contains the Features of sensor nodes in the network. It Consist of the sensor nodes and their behaviour.

Source ID	Destination ID	Route establishment	Enhanced Lion optimization scheme	Efficient path equalization routing	Enhanced LOEPRE scheme
2	**2**	**4**	**4**	**4**	**2**

Figure 2: proposed packet format

The packet format of proposed LOEPRE scheme is given in figure 2. 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 cross layer 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 cross layer against DOS attack. This field occupies 4 bytes. The last field is for enhanced LOEPRE scheme. This establishes the efficient path based on the node's energy. This field occupies 2 bytes.

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 protocols plans and coding can be reached in the absence of any unpredictability.

In our proposed method simulation, around 100 sensor nodes that go in the region of an 1100 meter X 950 meter square region with simulation time of 50 milliseconds. Mac address 802.11g is assimilated with design and all the nodes acquire fixed range of coverage of around 250 meters. The set up of simulation and its parameters are defined in table 1.

Table 1: Simulation setup of proposed protocol

No. of Nodes	100
Area Size	1100 X 950
Mac	802.11g
Radio Range	250m
Simulation Time	50ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	DSDV

PERFORMANCE ANALYSIS:

In simulation performance metrics using X graph in ns2.34 is analyzing

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 end most energy level. In proposed LOEPRE scheme it illustrates the reduced energy consumption when compared to other previous strategy EFCRS, SSPRA ELOER, EFLOR and TSTP.

$$\boldsymbol{Energy\ Consumption = Initial\ Energy - Final\ Energy}$$

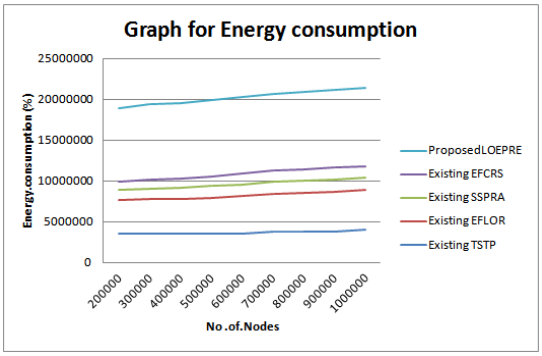


Figure 3: Graph for Number of Nodes Vs. Energy Consumption

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 sender node to sink node. In proposed LOEPRE scheme overhead in the communication is less when compared to other previous strategy EFCRS, SSPRA ELOER, EFLOR and TSTP.

$$Communicationoverhead = (NumberofPacketLosses/Received) * 100$$

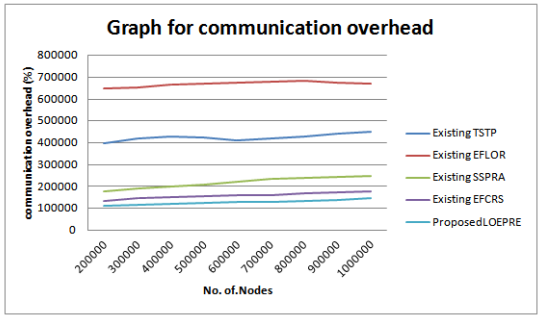


Figure 4: Graph for Number of Nodes Vs. Communication overhead

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 packet from sender node to destination node; every sensor node is created with the support of IP address. In the proposed LOEPRE scheme, end-to end delay is minimized when compared to other previous strategy EFCRS, SSPRA ELOER, EFLOR and TSTP.

$$EndtoEndDelay = EndTime - StartTime$$

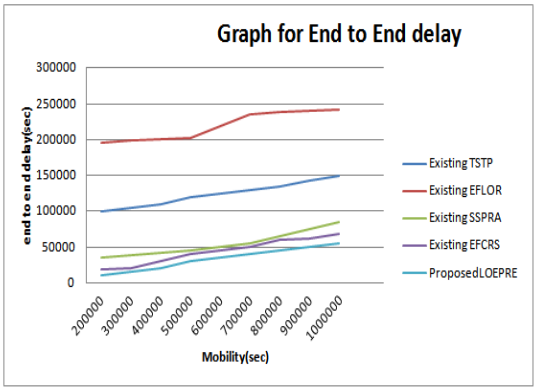


Figure 5: Graph for Time Vs. End to end delay

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

$$Detection\ efficiency = attackdetectionrate/overalltime$$

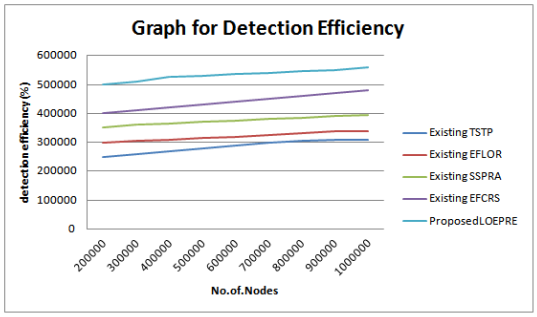


Figure 6: Graph for Nodes vs. Detection efficiency

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 high link stability when compared to

other previous strategy EFCRS, SSPRA ELOER, EFLOR and TSTP.

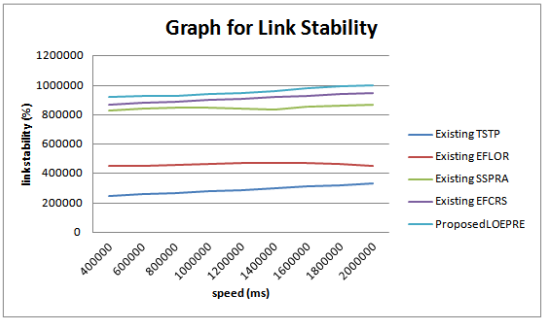


Figure 7: Graph for Speed Vs. Link Stability

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

$$Throughput = (Number\ of\ packet\ received/Sent) * speed$$

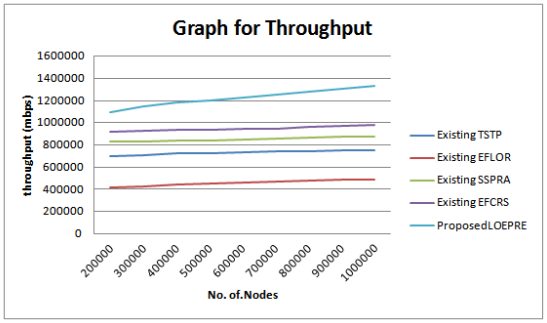


Figure 8: Graph for Number of Nodes Vs. Throughput

Packet delivery ratio: Figure 9 illustrates the comparison of packet delivery ratio that is analyzed by a measure of attainable packets from number of transmitted packets in specific speed. In the proposed LOEPRE method, packet delivery ratio is improved when compared to other previous strategy EFCRS, SSPRA ELOER, EFLOR and TSTP.

$$Packet\ Delivery\ Ratio = (Number\ of\ packet\ received/Sent) * speed$$

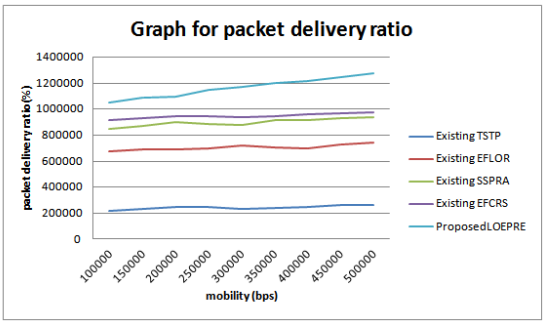


Figure 9: Graph for Mobility Vs. Packet Delivery Ratio

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

$$NetworkLifetime = timetakentoutilizenetwork / overallability$$

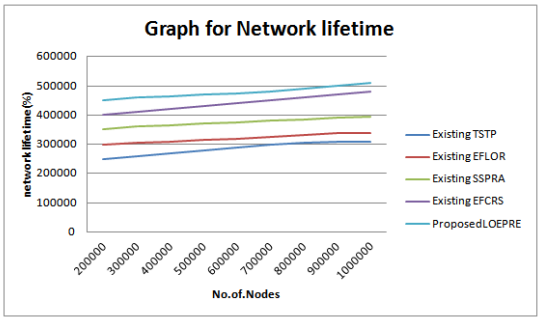


Figure 10: Graph for Nodes vs. Network Lifetime

CONCLUSION:

Enhanced lion optimization with efficient path routing equalization (LOEPRE) technique is proposed. To avoid DOS attack from cross layer 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 equalize path length in the network and is highly efficient. This technique is also used to reject the failure node in the cross layer 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 prolong network lifetime, minimum packet latency, reduces consumption of energy and achieves network lifetime. The simulation outcome of the proposed LOEPRE method highly robust while comparing to the existing methods EFCRS, SSPRA ELOER, EFLOR and TSTP. It achieves better performance than existing algorithms in comparing metrics connectivity ratio, end to end delay, overhead, network lifetime, throughput and packet delivery ratio.

CONFLICT OF INTEREST:

There is no conflict of interest.

FUNDING INFORMATION:

There is no funding information.

AVAILABILITY OF DATA AND MATERIAL:

There is no availability of data and material.

CODE AVAILABILITY:

There is no code availability.

AUTHOR'S CONTRIBUTION:

There is no author's contribution.

REFERENCES:

1. Cao, Y., Han, L., Zhao, X., & Pan, X. (2019). AccFlow: defending against the low-rate TCP DoS attack in wireless sensor networks. *arXiv preprint arXiv:1903.06394*.

2. Kanagasabapathy, P. M. K., Kedalu Poornachary, V., Murugan, S., Natesan, A., & Ponnusamy, V. (2019). Rapid jamming detection approach based on fuzzy in WSN. *International Journal of Communication Systems*, e4205.

3. Aborujilah, A., Nassr, R. M., Al-Hadhrami, T., Husen, M. N., Ali, N. A., Al-Othmani, A., & Ochiai, H. (2019, September). Security Assessment Model to Analysis DOS Attacks in WSN. In *International Conference of Reliable Information and Communication Technology* (pp. 789-800). Springer, Cham.

4. Krishnan, S. N. (2019). 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). Springer, Singapore.

5. Hafizullah, S., Verma, S., Vaidya, M., & Naugarhiya, A. (2019, March). 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). IEEE.

6. Iyer, S., Nadkarni, A. P., & Padmini, T. N. (2019, March). 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). IEEE.

7. Goyal, H., & Sharma, R. (2019). Performance Evaluation of Mobile Sink Using Metaheuristic Optimization Techniques. *Available at SSRN 3357806*.

8. Nuruzzaman, M. T., & Ferng, H. W. (2019). Design and evaluation of an LQI-based beaconless routing protocol for a heterogeneous MSN. *Wireless Networks*, 1-23.

9. Huan, X., Kim, K. S., Lee, S., Lim, E. G., & Marshall, A. (2019). A Beaconless Asymmetric Energy-Efficient Time Synchronization Scheme for Resource-Constrained Multi-Hop Wireless Sensor Networks. *IEEE Transactions on Communications*.

10. R. Kumar, 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

11. Chen, H., Liu, M., & Zhongchuan, F. (2019). Using Improved Hilbert–Huang Transformation Method to Detect Routing-Layer Reduce of Quality Attack in Wireless Sensor Network. *Wireless Personal Communications*, *104*(2), 595-615.

12. Thyagarajan, J., & Suganthi, D. K. (2019). A Novel Hybrid Opportunistic Scalable Energy Efficient Routing Design for Low Power, Lossy Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *11*.

13. Hussen, H. R., Choi, S. C., Park, J. H., & Kim, J. (2019). Predictive geographic multicast routing protocol in flying ad hoc networks. *International Journal of Distributed Sensor Networks*, *15*(7), 1550147719843879.

14. Venkateswarulu, B., Subbu, N., & Ramamurthy, S. (2019). An efficient routing protocol based on polar tracing function for underwater wireless sensor networks for mobility health monitoring system application. *Journal of medical systems*, *43*(7), 218.

15. Ang, L. (2019). Energy-efficient routing protocol based on tree route topology in wireless sensor networks. *The International Journal of Electrical Engineering & Education*, 0020720918822756.

16. Huamei, Q., Tao, J., Su, J., Zhiwen, Z., & Wangping, X. (2019). QoS adaptive and energy aware cross-layer opportunistic routing protocol in wireless

sensor networks. *IET Communications*, *13*(8), 1034-1042.

17. Wang, X., Zhou, Q., Qu, C., Chen, G., & Xia, J. (2019). Location Updating Scheme of Sink Node Based on Topology Balance and Reinforcement Learning in WSN. *IEEE Access*, *7*, 100066-100080.

18. Masood, M., Fouad, M. M., Seyedzadeh, S., & Glesk, I. (2019). Energy efficient software defined networking algorithm for wireless sensor networks. *Transportation Research Procedia*, *40*, 1481-1488.

19. Wu, K., & Liang, J. (2019, April). Path Planning in Mobile Wireless Sensor Networks. In *Journal of Physics: Conference Series* (Vol. 1187, No. 4, p. 042024). IOP Publishing.

20. Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). An Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN. *IEEE Access*, *7*, 135277-135289.

21. R P Premanand, A Rajaram, "Enhanced data accuracy based path discovery using backing route selection algorithm in MANET," *Peer-to-Peer Networking and Applications*, Sep. 2019. https://doi.org/10.1007/s12083-019-00824-1\

22. G Harikrishnan, A Rajaram, "Localization based optimizing Routing path against Attacks in Wireless Sensor Network, *International Journal of Computer Technology and Applications* (IJCTA), 9(10):97-110, 2016.

AUTHOR PROFILE:

R.Elavarasan completed his B.E degree in Electronics and Instrumentation Engineering in the year 2002 and Masters in Electronics and Control Engineering in the year 2009. He has been working as anAssociate professor at St. Joseph's College of Engineering in the department of Electronics and Instrumentation Engineering since 2007 and he has almost 9 years of experience in the respective field. He is currently pursuing Ph.D in Sathyabama University. His subject of interest includes Embedded Systems, Fiber Optics, Networking and his core research is on Wireless sensor Networks.

Currently Dr.K.Chitra is working as a Professor, School of Electronics Engineering, VIT University, Chennai. Dr. K. Chitra received her B.E. Degree in Electronics and Communication Engineering from Bharathiar University, Coimbatore in 1990, M.E. Degree in Applied Electronics from Bharathiar University in 1992 and Ph.D. degree in Optical Communication from Anna University Chennai in 2008. Dr.K.Chitra has spent her 25 years of experience in teaching and guiding projects for undergraduate and postgraduate students. Dr. K. Chitra has added 40 international publications to her credit. She has few funded projects from Government of India. Dr. K. Chitra's areas of interests include optical communication, optical networks, wireless sensor and computer networks, Biomedical Engineering and microwave Engineering.