I J C T A, 10(20), 2017, pp. 97-110 ISSN: 0974-5572

Localization Based Optimizing Routing Path Against Attacks in Wireless Sensor Network

G. Harikrishnan* and A. Rajaram**

ABSTRACT

Nowadays Wireless sensor network is vital role in different application, such as medical and military applications. Node senses the information and forwarded to sink or base station node in different path, forwarding packet get dropped because of injuries in path. Network lifetime not only depends on the energy during transmission, also consider injuries available in path. At same time node perform multiple tasks cause busy or hold the packet transmission in clustering technique. In this paper Localization based Optimizing Routing path (LORP) to increase packet delivery ratio, clustering with energy saving concepts available in network. The virtue based authentic nodes are selected to optimize the effective routing, energy to limit the many packet transmission at same time. Overload occurred are detected and changing path to another cluster depends on the ability of nodes. Only accept the packets from virtue nodes in network. Normally clustering causes no side effects, to reduce packet latency.

Keywords: Localization based optimizing routing path, clustering, virtue based authentic nodes, optimizing virtue node Routing path, trustworthiness.

1. INTRODUCTION

Nowadays wireless devices are minimized it size based on incorporated sensing, calculation and message passing capacity. Wireless sensor network designed by many integrated devices is used in several applications. Mostly used in security applications like military, civil, and scientific areas. These applications contain security inspection, digital battleground, forest flames, factory floor mechanization, habitat analyzing. WSN contains group of sensor link environment and split information's direct to measure the amount of assured notice. The combination of packet of many nodes reward for the packet drops in forwarding individual sensors and activates improved truth. An important model of uses in the area of infrastructure monitoring then it analyzes the current condition of roads, pipes, large bridges [1]. Sensor suggests unmatched ability in given that permanent sensing of important areas.

Multi-transceiver mechanism was respectively functional to wireless sensor network for increasing network routine. Due to the incomplete objective capability of sensor node, and it is not easy for wireless sensor to directly design multi-transceiver mechanism on the sensor network. Supportive communication methods could be best to attains similar performance to multi- transceiver system in WSNs. MIMO- Virtual multi-input multi-output cooperative method is presented [2]. Survey the energy effectiveness of cooperative MIMO sensors networks with recognized that MIMO systems are more energy-efficient than SISO-single-input single-output method for lengthy space between two channel communications. The sensible resource optimization in a cooperative network can additional enhances the performance of network. It is previously proved allocation of resource is capable to reduce the total energy use with both the transmission energy and network active state energy usage.

* Department of Electronics and Communication Engineering, Research Scholar, SCSVMV University, Kanchipuram-631 561.

** Professor, Department of Electronics and Communication Engineering, EGS Pillay Engineering College, Nagapattinam-611002.

Optimal control allotment method that reduces the transmit authority was implemented with a limit on the average BER performance for MISO virtual multiple-input single-output supportive communication in wireless sensor [3]. In present analyzed optimal and some efficient suboptimal control allocation in sensor with out of coverage range. The optimal power allocation in [4] was proposed as a closed-form report for EE maximization by solving KKT-Karush-Kuhn-Tucker conditions in a downlink MISO distributed transceiver method. An efficient resource allocation algorithm is presented by using fractional programming to availably enhance EE in OFDMA methods with large number of base station transceiver. Then additionally minimize the computational difficulty, minimum difficulty resource share and SDMA -scheduling algorithms for downlink space-division multiple access method is proposed [5].

In other mode, the identified node deployment method use civil applications like as environment monitoring location of nodes can be filtered to attain an overall network goal. Location of sensor nodes considerably influences process of a network. Accept the optimization goal factor in important performance parameters like lifetime of network, connectivity and coverage [6]. Many of these parameters have been embattled by existing survey. A broad range of characters have been measured with the energy efficiency of the data transmission, medium access intrusion, radio coverage range, and packet latency. A general surveillance about previous work is the centre on polygon-based, normal and abnormal, with minimum attention given to linearly-shaped environment.

Remaining of the paper is planned as follows. Section II indicates a related works. In section III, we present the details of proposed Localization based Optimizing routing path (LORP) provides localization based virtue node optimized routing path. Section IV provides simulation performance results analysis obtained under different parameters. Finally section V concludes the paper with future track.

2. RELATED WORKS

Xia Lei1 et al., [9] proposes an optimization of Monte Carlo mobile node localization algorithm depends on minimum squares correct. The node route is forecasted by using the least-squares fitting mechanism, the node load data used to evaluate the unknown nodes. The simulation report indicates in which distinguish with the traditional schemes, the Location accuracy of the algorithm is considerably increased. Depends on the investigation of the usual locationing algorithm and the Monte Carlo mobile node localization, the paper analyze the method of minimum squares appropriate algorithm to forecast the node stability tendency, and to decide the sampling gap. In a certain range, the present algorithm can improve the correctness of the unknown nodes in network.

Amel Berrachedi et al., [10] proposed denotes the issues of sensor network must be implemented to have high-quality performances in particular the energy usage and the packet drop. Use communicative type of Petri Nets also known as Deterministic Stochastic Petri Nets. It indicates the applicability of the present model; one of routing methods enthusiastic for WSNs. Calculated the energy usage and the packet drop using formalisms depends on the Petri Nets. Then Deterministic Stochastic Petri Nets because they appear more suitable to our difficult. Direct to demonstrate the behavior of the present DSPN model and evaluated these two parameters, best of the commonly present outputs for WSN packet forwarding called constant grouping. Simulation result indicates in which CHs use significantly energy relative to associate nodes. In additionally there is minimum packet drop.

Thi-Nga Dao et al., [11] present various applications need that used energy is reduced and packets are transmitted to the sink within a time period. Direct connection with packet delay issue, there has been various previous methods in clockwise process WSNs other than they need time organization or maximum message difficulty. All of them at rest cause increase packet delay. So, present sub-interval based scheduling algorithm that goals to improving average packet delay in clock cycle WSNs. By transmission earlier sub-gap for nodes that can make longer progress among potential transmitters, packet delay should be minimized considerably. Mathematical report indicates that sub-gap based scheduling algorithm to attain minimum delay than DASF. Present sub-gap based scheduling algorithm to minimize packet latency. In sub-interval scheduling algorithm, nodes that are earlier to the sink in the middle of possible forwarders are assigned earlier sub-gap. Network simulation report indicates that sub-gap algorithm can increase latency performance compared to DASF in network infrastructure.

Prasanta Kumar Swain et al., [12] present a easy investigative model to identify Quality of Service (QoS) parameters for estimating packet loss in terms of probability of jamming. Designing a simple buffer state in the MAC layer function, to reduce loss of packet can be compressed format, in which reduces the energy consumption for retransmission of information. Last QoS parameters like before time for data packets, enhance the system deployment are also strong-minded to estimate system presentation. Packet over load model for WSNs. QoS parameters in terms of likelihood of jamming, increase waiting time in queue is resolute. The next check unit facilitate with a buffer of single storage space capacity to compensate the waiting time for output of first service unit till availability. As per the suggested mode a trade off between jamming of data packets and checking rates must be selection.

Shilpa Katikar et al., [13] presents a little the data rate is maximum. Over load in multi-hop wireless sensor network is not dispersed consistently among the nodes so there are many probability of dropping packets. Then avoid this drop a needed performance should be occupied. A caching method is one of that with which drop packets can be gathered and retransmitted to end node, in which attains reliability and to improve the performance of network. In active state is not target. Subsequently, it presents the mathematical examination of the fixed characteristics. Time slots contains a passing mathematical study for DSPNs by selecting an implementation latency revival scheme uses caching method to achieve minimum packet drop and improves reliability of network. It denotes describe above address the Loss revival in transmission. Drop rate is with loss revival model minimized, and enhancing packet delivery ratio this success happens with similar energy level to increase network lifetime.

Ashish Thomas et al., [14] present survey of attack known as JF-Jelly Fish Attack. Injuries can exploit the inbuilt weakness of network. Watchful learn brings into centre the dangerous attack spot that can be broken in the previous multicast routing protocols, it is very strong and protected algorithm has to be implemented. To created and analyzed the crash of a jellyfish shuffle attack and present a mechanism to avoid such an attack on ODMRP routing protocol for network. It is used Multicast routing protocol with the aid of criterion network simulator known as Exata-Cyber security. Network simulator uses a mixture of network and UAV network that allocating ODMRP protocol to take out a JF shuffle attack and it removed. Then also optional mechanisms to ease a shuffle JF attack on a UAV/mobile networks. Paths are selected in reliable manner. This mechanism add a attacker node of network, thus make the network highly protected and trustworthy.

Sunitha et al., [15] proposed an OCAEE-LB optimized congestion aware energy efficient traffic load balancing mechanism for packet forwarding in WSN. This method use the ignored information during path finding procedure with considers a compound routing parameters to decide injuries status of a node and to put into effect the traffic load balancing method. It is simulated by *ns-2* results show that the present method process better than the previous AODV-LB algorithm of different performance parameters like, network overhead, bandwidth, throughput, packet latency, energy usage, and traffic occurrence. Sender node choosing many paths for data transmission then, quality of service estimated for different WSN uses. Each the exchange paths are followed in routing table and best three paths are chosen for data transmission. Minimum number of path is stored in the routing table to minimize the storage and overhead.

Xin Yang, et al., [16] proposed to implement a routing protocol for uses over minimum authority and LLNs-lossy networks, the IETF ROLL Working Group standardized the IPv6 RPL-Routing Protocol for LLNs that collect nodes in a LLN into a tree-like topology known as DODAG-Destination Oriented Directed

Acyclic Graph connectivity in environment. The High-quality scalability and quick access network deployment. Then, it affects from cruel untrustworthiness due to choose suboptimal paths with minimum quality connections. To optimize the dependability of RPL paths, presents strength of parameters depends on routing protocol denoted as RPL for reliable transmission and LLNs gathers data. Launch a latest routing parameters for RPL known as SI-stability index that exploits strength description of RPL nodes to choose more steady paths. In addition, proposed a passive and lightweight network layer method to calculate the bi-directional ETX-expected transmission count for LL-wireless links.

Avani Sharma et al., [17] present attack; the malicious node contains itself in path to target and intermediate nodes in data transmitting. Then, the malicious node provides latency for data packet when transmitting in up direction. The characteristics of malicious node spoil transmission rate. Result of JFDV attack with automatic protocol has been considered in existing literature. Monitor the result of JFDV attack using both automatic and proactive protocols. Analyze the characteristics of proactive protocols make them opposing to JFDV attack as distinguish to automatic protocols. Estimate JFDV –Jelly Fish Delay Variance attack with reactive method, AODV to authenticate reports of existing method. Estimate effect of attack with various latency of time and fraction of attacking nodes on PDR of network. That the attack has upsetting impact on the transmission rate of TCP flows with maximize in latency time and with part of attacking nodes.

Kaiyue An et al., [18] proposed brute force mechanism depends on optimal power scheduling method can maximize Effective energy with power constraint, and the optimal power scheduling in closed form report by solving Lagrangian process. Then minimize additional difficulty, the greedy node chosen also included. At last, arithmetical report indicates that the present greedy node chosen mechanism can get the routine approximately the same to the brute force mechanism in simulation. The joint optimization of node chosen and power scheduling for supportive transmission in wireless sensor networks as a non-convex optimization issues, anywhere the network power debauchery and lesser count of active nodes are occupied into concern. An optimal power scheduling mechanism in brute force method is presented by Lagrangian process that increases the energy efficiency for virtual MISO scheme. Also minimize the computational difficulty, the greedy node selection. This algorithm converges within a minimum number of iterations, but also unveil that estimate performance is almost same to the precise results evaluated in brute force mechanism.

Pedro Pinto et al., [19] present RA-EEDEM, a group of modification made to RPL that enhance the EED End-to-End Delay estimation accuracy. The RA-EEDEM changes include changes to the RPL parameters and to its Objective Function (OF). The report indicates in which RA-EEDEM enhance the correctness of EED estimation while reducing its impact on the average EED and PRR -Packet Reception Ratio. Present RA-EEDEM that contains a set of changes to RPL aimed to improve the EED estimation correctness. RA-EEDEM distinguish a new parameters and changes to the OF mechanism. RA-EEDEM evaluate reports are distinguish against our existing calculation output EEDEM and a ETT-based answer. The report indicates that RA-EEDEM improves the correctness of the EED view when distinguish to the other outputs.

Vishal Monga et al., [20] present principled algorithmic mechanism to merge the advantages of these two complementary methods. The cost process does not show joint convexity over the multidimensional variable group of node position and matching result values that make this optimization particularly demanding. It makes two important aid: first the case of simplex interruption, a cost function is formulate that exhibits independently convexity in its influence and activates an efficient uneven curved optimization algorithm, and Next the abovementioned structure, for fixed node results, the optimization of node positions is opening into a primary and an supplementary optimization that greatly enhances the quality of the result over traditional alternative anywhere node positions are straight optimized. Initial simulation indicates significant improvements in color transform accuracy over available optimizing just the node locations or output values. The surveillance that joint optimization of LUT nodes and result is better to separate optimization of either quantity only. The formulation of a cost function that exhibits divisible Convexity with respect to the weighting matrix, resolute only by node position and the vector then For fixed process, the derivation of via a constrained convex optimization in conjunction with an supplementary Lagrangian optimization to make sure a that induce by actual node position in network.

3. OVERVIEW OF PROPOSED SCHEME

In Wireless sensor network which find the attack and remove using virtue based authentic nodes. Maintain the stability of each nodes present in network environment. Packets overload in particular node receiving time, affects the overall performance such reduce network lifetime. Localization based Optimizing Routing path optimize the effective routing path. Localization denotes the node deployment among network, nodes have different characteristics to perform packet loss that are monitored and removed from entire network.

Figure 1 shows Localization based optimizing routing path against attack clustering the nodes routing the packet in different path get packet loss, so select virtue based authentic nodes in network, establish the efficient communication between sources to cluster heads with localization of network environment. Identify jellyfish attack and removed from network use optimization to achieve efficient routing path to reduce packet overload and also minimize packet latency.

3.1. Localization based normal routing

Localization technique to monitor larger area network with using sensor to attains effective routing. This method focus the packet latency, during transmission there is packet overload occurred. Clustering the

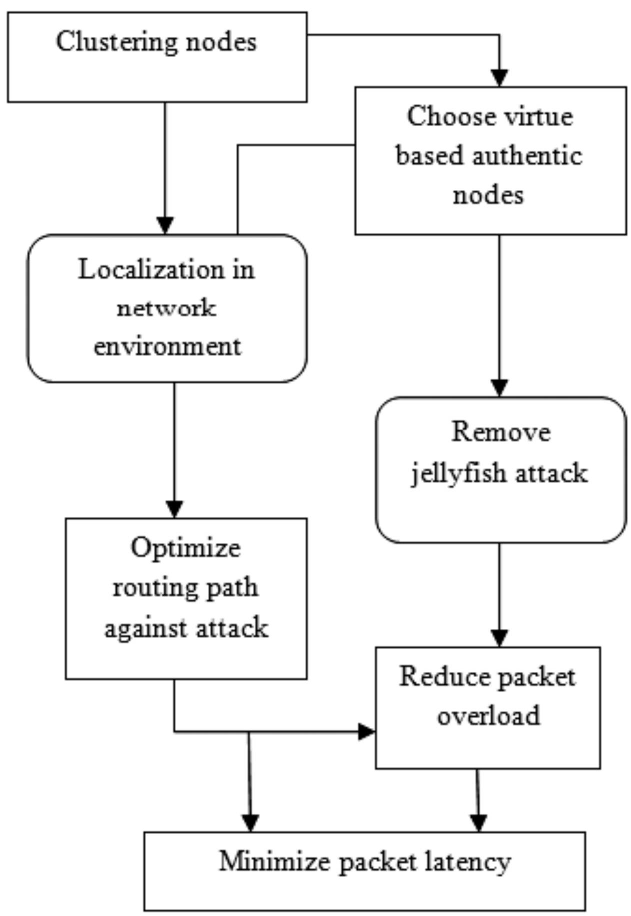

Figure 1: Block Diagram of Localization based optimizing routing path against attack

entire network to split nodes form different clusters depends on energy availability of each node and bandwidth. Nodes not contains same energy level, nature of node energy is varied. Sometimes energy depletion is made the cause packet drop.

Nodes in network is not updating position every time it does not random movement so energy usage is reduced, but sensing process all node consumes more energy. Normally nodes transmit packets in orderly first in first out manner, so it creates the queue in waiting stage of each packet. Node must transmit packet in every slot period exceed that time overload occurred in each transmission. Whether any node loss its energy, because of overload in communication among nodes in clusters. Jelly fish attack is like a denial of service attack and also a type of inactive attack is not easy to identify entire network environment. It provides latency in transmitting and receiving packets. Node should establish the efficient connection to overall network, connectivity searching process is going up to reaches trustable path routing.

Organize sensor nodes into normal numerical patterns and make sensor nodes deployed in the network. The relative positions of sensor nodes stay the same during the movement. Thus, unknown nodes can estimate their locations depending upon received signal strength and numerical relationship of the sensor nodes. Base station gives connection for communication holding nodes; it takes more time, because t is in already waiting packet transmission. Cluster head collects the data packets from its non cluster node and finally it uploads the packet to base station.

In uploading process nodes are maintain a reliable connection, so provide an attack free routing path. It changes the route path to efficient route path for every transmission in wireless sensor network. Base station checks packet is in ordered form or non ordered form to localize the normal routing to base station node. It controls the cluster node and non cluster head in coverage area in network. Sufficient size of packet is only allowed in each cluster; otherwise go to next and so on.

3.2. Monitoring and removing jelly fish attack in wireless network

Sensor nodes communicate with each other based clustering method there is an attack involved in the process. In communication time packets send from source node, intermediate cluster members drop the packet randomly by the jelly fish attacker. Attacker change information and then transmits to next neighbor node in non cluster node or cluster member node. Therefore, data packets are re-transmitted, until it attains reliable transmission path achieving. n_{weig} is computed as:

$$n_{weig} = Rt_m * S_p \tag{1}$$

Where R_{tm} is routing table message, n_{weig} is weight of the node, and S_p sender packet size. In transmission use virtue based authentic node in all clusters, cluster head collect each node packets, after analyzing packet, missed packet, latency packet, and reordered packets are detected and use retract mechanism, cluster member nodes collects data packet information in backward manner. So cluster head node evaluates the jelly fish attacker node. In jelly fish attacker node behaves in three categories they are reorder packet information, latency in packet delivery, and packet dropping.

Source node forward packet to intermediate cluster node if it is a faulty check the coverage; establish the efficient connection for all cluster member nodes. Nodes having different activity, so it cause attacks like packet drops and mainly focus on latency for packet transmission, packets should delayed in every transmission because of over load the time slot allocation is varies for each clusters depends on size of packet. Those types of information's are maintained in routing table viewed by cluster head and base station nodes. Where $En(p)$ ending node path, $Sn(p)$ starting node path n_{dis} is computed as:

$$n_{dis} = En(p) - Sn(p) \tag{2}$$

Source node s measures the cluster member node distances between each other n_{dis} and weight of the node n_{weig} for n transmission between first cluster nodes in wireless sensor network. S_g is computed as:

$$S_g = \left(\frac{\left(n1_{dis} * n1_{weig} + n2_{dis} * n2_{weig} + n3_{dis} * n3_{weig} \right)}{C * t} \right) \tag{3}$$

Where c is communication between neighbor nodes available in a path and t is time taken for complete process. Where denotes virtue based authentic nodes. v is computed as:

$$v = \left(1 - n_{dis}\right) * \left(1 - n_{weig}\right) * s_g \tag{4}$$

$$v = \left(1 - n_{dis} * n_{weig}\right) * s_g \tag{5}$$

$$v = \left(1 - n_{dis} * n_{weig}\right) * s_g \left|p\right| \tag{6}$$

$$C_o = 1 - n_{dis} * n_{weig} \tag{7}$$

$$v = c_o * s_g \left|p\right| \tag{8}$$

Virtue based authentic nodes are used to design a routing path with different clusters available in wireless sensor network. Where C_o indicates each node distance and each node weight. So, virtue mechanism obtains the minimum distance and efficient routing path in network. Accept only virtue node; reject the nodes like packet dropping, packet latency, and packet modified attacks during transmission. Move the nodes to out of coverage region among the network environment. Remove that kind of jelly fish attack, to reduce energy consumption for entire network areas.

Clustering with virtue based authentic nodes selection algorithm

Step 1: for each Data packets S_p then

Step 2: if *neighbor node* == Rt_m

Then forward packet to neighbor node

Step 3: n_{weig} all neighbor node weight is calculated.

Step 4: n_{dis} distance between intermediate nodes are estimated.

Step 5: else there is no coverage.

Step 6: end if.

Step 7: *S*tarting node to ending node Time for routing = *En*(*p*) – *Sn*(*p*) + *delay* time.

Step 8: S_g forward $S_g |p|$ to it's cluster head node.

Step 10: each node distance are calculated by c_o.

Step 11: v virtue nodes are identified.

Step 12: End for.

3.3. Optimizing virtue node Routing path

In optimization, node present in the network need to forward packets for its requirements. They transmit packet to intermediate neighbor to neighbor then to cluster head, they select only optimized virtue node routing path from different source node to different cluster head. Cluster members select the node in energy based manner with resource allocation. The speed of packet transmission in virtue node, worthy of node activities are analyzed then after check minimum count of nodes available in routing path or not, and it possible to discover other position of nodes in cluster group that improves the network overall trustworthiness. In proposed Localization based Optimizing Routing path (LORP), monitor the issues like jelly fish attack during packet transmission they also removed from cluster group to out of coverage stage.

$$\textit{forward packet}(v) \tag{9}$$

$$\textit{forward packet}\ (v, c_o * Sg|p|, \textit{trustworthy}) \tag{10}$$

This method optimizing the trustworthy path for cluster member node communication it enhances the packet delivery ratio, reduce packet drop and latency, because the injuries are detected and removed that goes to inactive state in wireless network. Inactive state of node causes no side effects in packet transmission, the injuries are detected and optimized routing path is selected to attain effective communication, there is no packet overload occurred for during transmission time so latency of packet delivery is reduced.

Algorithm for optimizing virtue node routing path

Step 1: If path checks the resource utilization for transmission then

Step 2: Add path ($s_g|p|$, Rt_m)

Step 3: check trustworthiness of nodes.

Step 4: *Trust path* (*node*) == *rtable* (*node*) then

Step 5: *Trustworthy* (*n*) = *rtable* (*path weight*) + *T* + *v*

Step 6: optimized virtue node routing analyzed. forward packet (v, c_o*S_g|p|, trustworthy)

Step 7: else delete path *(node).*

Step 8: end if

In Wireless sensor network establish efficient communication among the cluster members based on virtue node with high trustworthiness until packet reaches to base station, that controls all cluster head and cluster member nodes. The quality of packet evaluation from a group of homogeneous cluster members, it is worth. So, selects the optimized routing path with trustworthy node.

Packet ID: Packet ID contains all wireless sensor node information's. It furthermore has node's position and node behaviour analysis in network area.

In figure 2: the proposed packet format is shown. Here the source and destination node ID field takes 2 bytes. Third one is Clustering nodes contains 4 bytes. Simulator establishes the grouping of nodes based on energy and bandwidth. In fourth field occupies 4 bytes. Localization of nodes monitored it deployment and activity node. In fifth occupies 4 bytes, the virtue based authentic node, only select the efficient node and remove jelly attack nodes. The last filed Packet forward for Trustworthy, it optimize the routing path based on trustworthy occupies 2 bytes, to classify wireless sensor nodes.

Source ID	Destination ID	Clustering nodes	Localization of nodes	virtue based authentic	Packet forward for Trustworthy
2	2	4	4	4	2

Figure 2: Proposed Packet format

6. PERFORMANCE EVALUATION

6.1. Simulation Model and Parameters

The proposed LORP is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 sensor nodes deployed in 1050 meter × 900 meter square region for 80 milliseconds simulation time. All sensor nodes deployed in random manner among the network. All nodes have the same transmission range of 250 meters. CBR Constant Bit Rate provides a constant speed of packet transmission in network to limit the traffic rate. DSR Dynamic source routing protocol is used to assign optimized path for packet transmission. Table 1 shows Simulation setup is Estimation.

Table 1
Simulation Setup

No. of Nodes	100
Area Size	1050 × 900
Mac	802.11
Radio Range	250m
Simulation Time	80ms
Traffic Source	CBR
Packet Size	150 bytes
Mobility Model	Random Way Point
Protocol	DSR

6.1.1. Simulation Output

Simulation Result: Figure 3 show that the proposed LORP method monitors and detects jelly fish attack with different combination in efficient manner compared with existing MANAL [7] and CNPO [8]. LORP localizing the node in wireless network, to identify nodes categories is attacker or trusty node use virtue based authentic node selection method to attains optimized routing path.

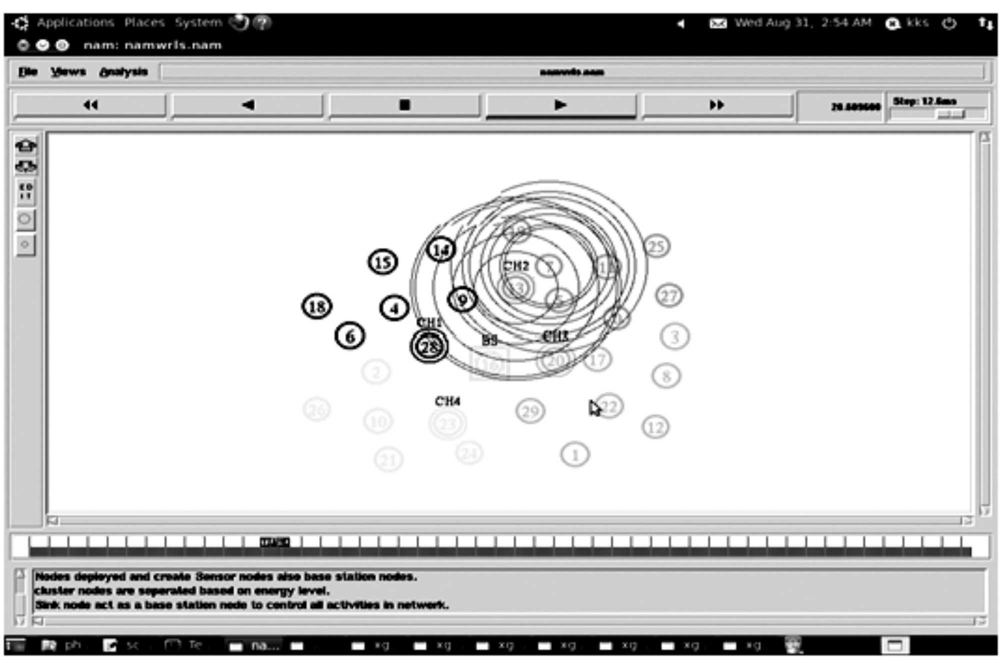

Figure 3: Proposed LORP Result

6.1.2. Performance Analysis

In simulation to analyzing the following performance parameters are using X graph in ns2.34.

Packet Latency: Figure 4 shows packet latency is estimated by amount of time used for packet transmission from source node to destination node, all node connectivity stored by node buffer. In proposed LORP method packet latency is reduced compared to Existing method NARP, MANAL, and CNPO.

Packet latency = End Time – Start Time

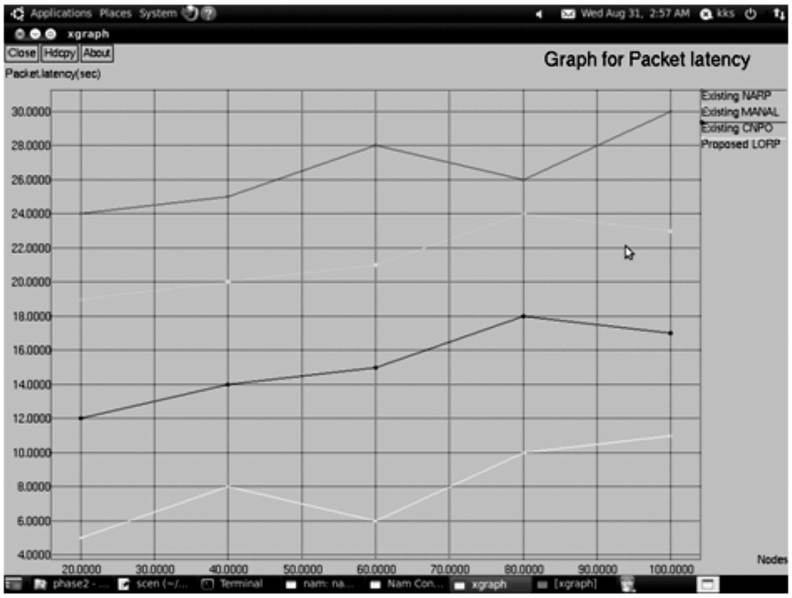

Figure 4: Graph for Nodes Vs. Packet latency

Communication overhead: Figure 5 shows communication overhead is minimized in which source forward packet to intermediate node, optimized routing method provides trusty path for packet transmission. In proposed LORP method communication overhead is minimized compared to Existing method NARP, MANAL, and CNPO.

***Communication overhead = (Number of Packet Losses/Receivede)* * 100**

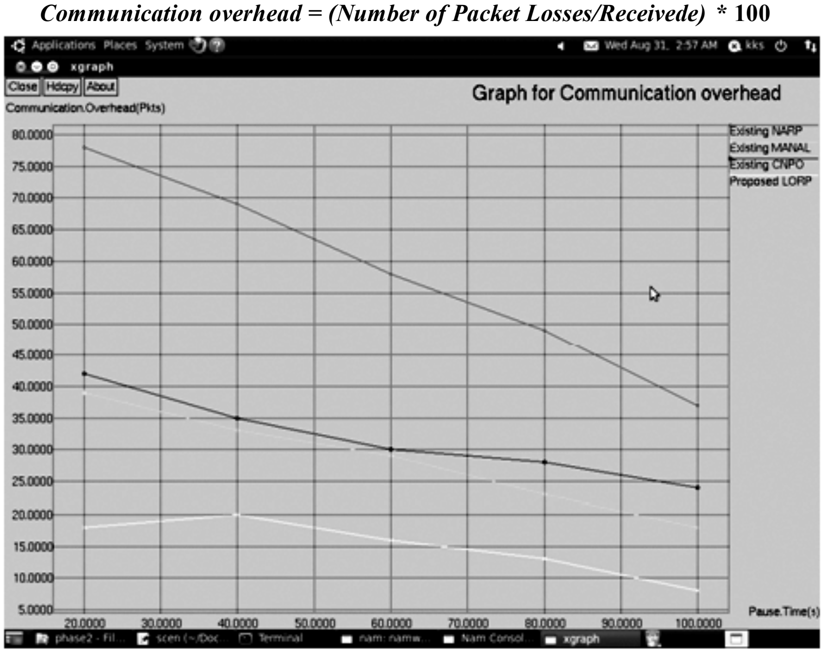

Figure 5: Graph for Pause Time Vs. Communication overhead

Packet Delivery Ratio: Figure 6 shows Packet delivery ratio is measured by packet received count from packet sent count in particular rate. Node velocity is a constant in sensor network; simulation rate is fixed at 100. In proposed LORP method Packet delivery ratio is enhanced compared to existing method NARP, MANAL, and CNPO.

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

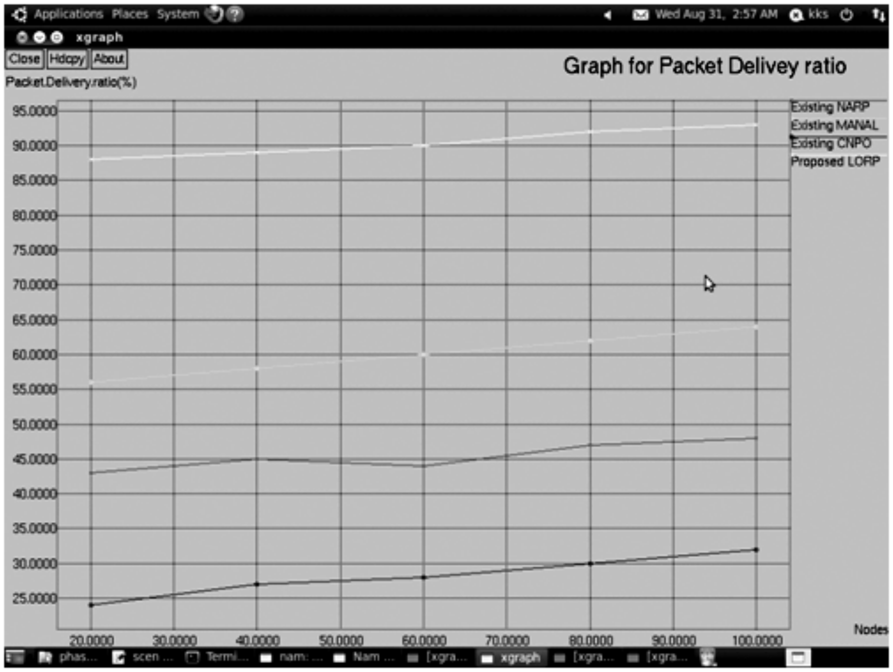

Figure 6: Graph for Nodes Vs. Packet Delivery ratio

Network Lifetime: Figure 9 show that Lifetime of the network is calculated by entire process of network, effort utilized to done communication successfully.In proposed LORP method Network Lifetime is Enhanced compared to Existing method NARP, MANAL, and CNPO.

Network Lifetime = length of emergy usage/overall energy

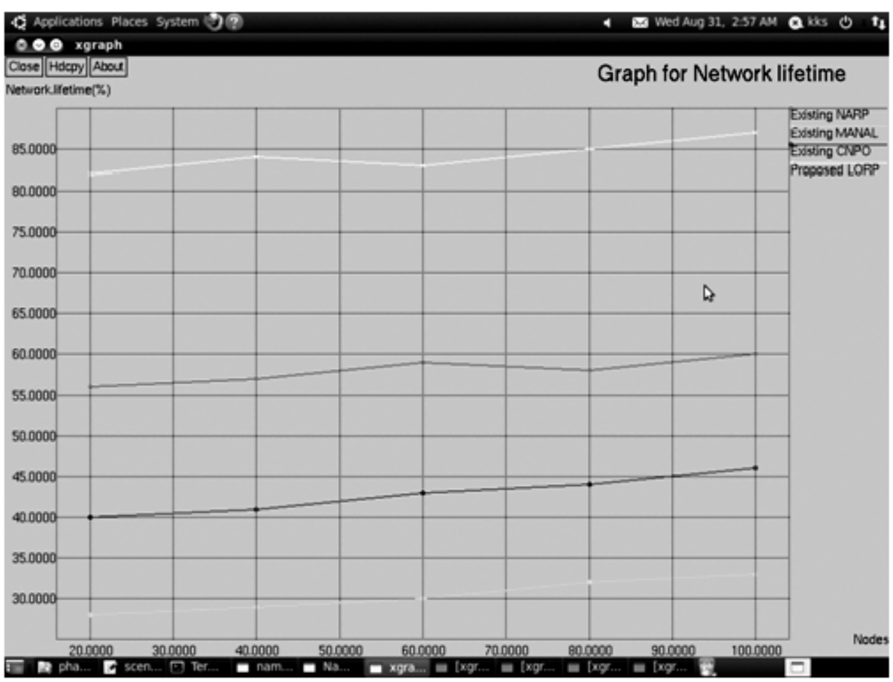

Figure 7: Graph for Nodes Vs. Network Lifetime

Energy Consumption: Figure 8 shows energy consumption; evaluate total energy used for starting node to ending node. In proposed LORP method virtue based authentic nodes are used for packet transmission so energy consumption is minimized compared to Existing method NARP, MANAL, and CNPO.

Energy Consumption = Initial Energy – Final Energy

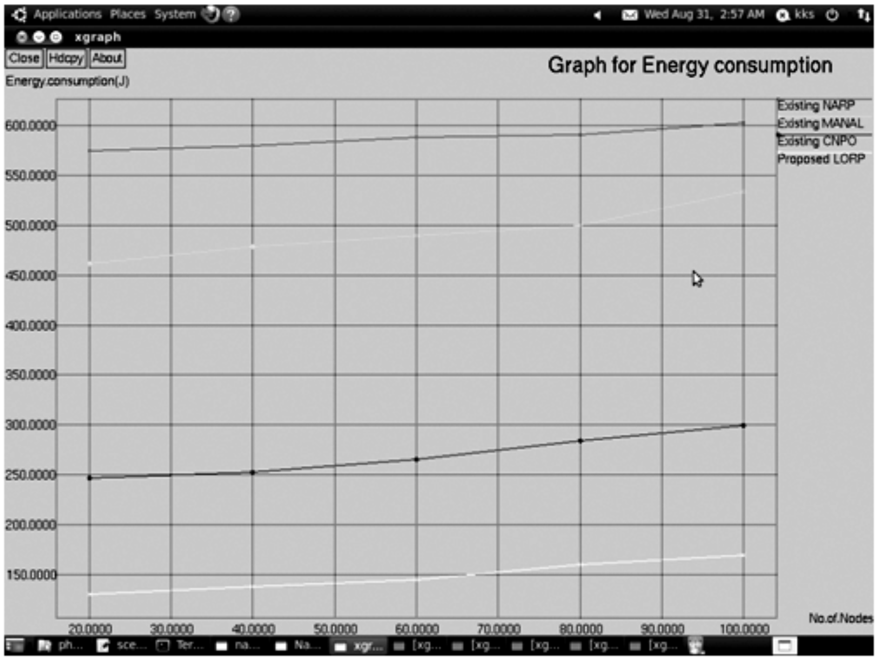

Figure 8: Graph for No. of Nodes Vs. Energy Consumption

Packet drop rate: Figure 9 show that Packet drop of all communication in network is planned by nodes drops the packet because of overload so use virtue node it is efficient node to select routing path in effective manner. In proposed LORP method Packet drop rate is minimized compared to Existing method NARP, MANAL, and CNPO.

$$Packet\ drop\ rate = \left(Number\ of\ packet \frac{dropped}{Sent} \right) * 100$$

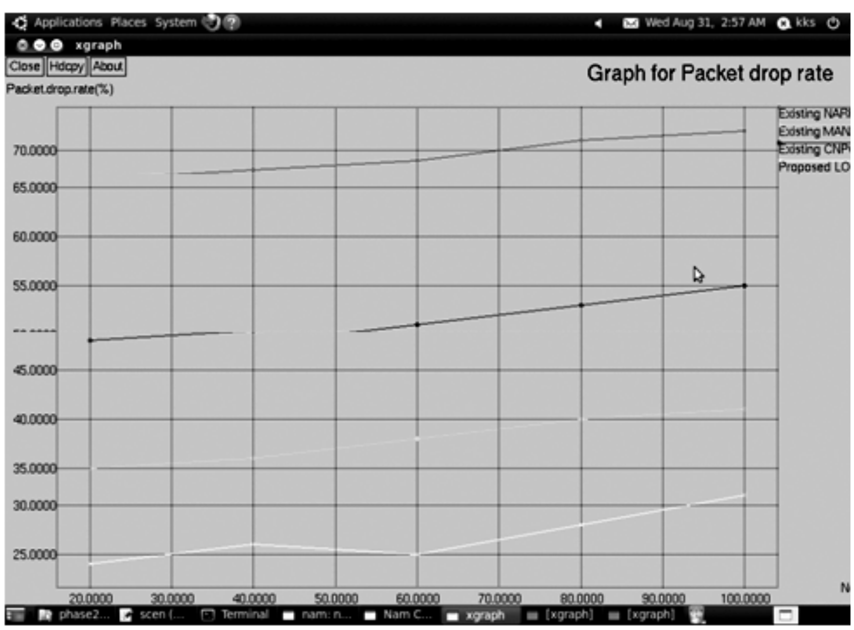

Figure 9: Graph for Node vs. Packet drop rate

7. CONCLUSION

A wireless sensor node contains clusters; clustering the sensor depends on its node capacity. Nodes sense the information and forward that data packet to cluster head and then to base station in network. In cluster member processing attacks involved to affect the packet forwarding, jelly fish attack causes packet latency, packet modified, and packet drops. Proposed LORP method to monitor and remove the attacker node for out of coverage range. Virtue based authentic node is used to detect all nodes trustworthiness, trust nodes are enable in network processing time, non trusty attacker nodes are disable because it consume more energy. Only trusty nodes are selected to optimize the efficient routing path, it minimizes energy consumption, packet latency, and packet drop rate. In future propose Real clustering with enhanced fuzzy to analyze various parameters in different stage of sensor nodes in network.

REFERENCES

[1] I. Jawhar, N. Mohamed, and K. Shuaib, "A framework for pipeline infrastructure monitoring using wireless sensor networks," Proc. of the Wireless Telecomm. Symp. (WTS 2007), New York, NY, April 2007.

[2] S. Cui, A. J. Goldsmith, and A. Bahai, "Energyefficiency of MIMO and cooperative MIMO techniques in sensor networks," IEEE J. Select. Areas Commun., vol. 22, pp. 1089-1098, Aug. 2004.

[3] H. Wan, J.-F. Diouris, and G. Andrieux, "Power allocation for virtual MISO cooperative communication in wireless sensor networks," in Proc. IEEE Wireless Technology Conference, Paris, France, Setp. 2010, pp. 69-72.

[4] H. Kim, E. Park, H. Park, and I. Lee, "Beamforming and power allocation designs for energy efficiency maximization in MISO distributed antenna systems," IEEE Commun. Lett., vol. 17, pp. 2100-2103, Nov.2013.

[5] Kai, S. U. N., W. A. N. G. Ying, and Ping ZHANG. "Low complexity resource allocation and scheduling algorithms for downlink SDMA systems." The Journal of China Universities of Posts and Telecommunications 16.5 (2009): 33-40.

[6] M. Younis and K. Akkaya, "Strategies and Techniques for Node Placement in Wireless Sensor Networks: A Survey," The Journal of Ad-Hoc Networks, Vol. 6, No. 4, pp. 621-655, 2008.

[7] Han, Guangjie, et al. "A Survey on Mobile Anchor Node Assisted Localization in Wireless Sensor Networks." (2016).

[8] Alduraibi, Fahad, Noureddine Lasla, and Mohamed Younis. "Coverage-based Node Placement Optimization in Wireless Sensor Network with Linear Topology." IEEE ICC 2016 Ad-hoc and Sensor Networking.

[9] Lei, Xia, Tan Zhi, and Liang LiWen. "Optimization of Monte Carlo mobile node localization algorithm based on least squares fitting." 2016 Chinese Control and Decision Conference (CCDC). IEEE, 2016.

[10] Berrachedi, Amel, and Malika Boukala-Ioualalen. "Evaluation of the Energy Consumption and the Packet Loss in WSNs Using Deterministic Stochastic Petri Nets." 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2016.

[11] Dao, Thi-Nga, and Seokhoon Yoon. "A sub-interval-based scheduling algorithm in duty-cycled wireless sensor networks." 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2016.

[12] Swain, Prasanta Kumar, and Manas Kumar Rath. "Analysis and QoS measurement for voluminous data flow in Wireless Sensor Network." 2016 3rd International Conference on Recent Advances in Information Technology (RAIT). IEEE, 2016.

[13] Katikar, Shilpa, and Vivek Deshpande. "Reliability enhancement in WSN using loss recovery model."2015 International Conference on Information Processing (ICIP). IEEE, 2015.

[14] Thomas, Ashish, Vijay Kr Sharma, and Gaurav Singhal. "Secure Link Establishment Method to Prevent Jelly Fish Attack in MANET." 2015 International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2015.

[15] Sunitha, G. P., BP Vijay Kumar, and SM Dilip Kumar. "Optimized congestion aware energy efficient traffic load balancing scheme for routing in wireless sensor networks." 2015 International Conference on Information Processing (ICIP). IEEE, 2015.

[16] Yang, Xin, et al. "Stability metric based routing protocol for low-power and lossy networks." 2014 IEEE International Conference on Communications (ICC). IEEE, 2014.

[17] Sharma, Avani, Rajbir Kaur, and Purnendu Karmakar. "JFDV Attack: Influence on Workability of Mobile Ad-Hoc Networks." Computational Intelligence, Communication Systems and Networks (CICSyN), 2014 Sixth International Conference on. IEEE, 2014.

[18] An, Kaiyue, et al. “Joint optimization of node selection and power allocation in wireless sensor networks.” 2014 12th International Conference on Signal Processing (ICSP). IEEE, 2014.

[19] Pinto, Pedro, António Pinto, and Manuel Ricardo. “RPL modifications to improve the end-to-end delay estimation in WSN.” 2014 11th International Symposium on Wireless Communications Systems (ISWCS). IEEE, 2014.

[20] Monga, Vishal, and Raja Bala. “Algorithms for color look-up-table (LUT) design via joint optimization of node locations and output values.” 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2010.