DSR Protocol using Multiple Node Based Particle Swarm Optimization (MNPSO) Congestion Aware Algorithm in Wireless Sensor Network

J.Saranya [1] **and** ***Dr.P.Bharathisindhu*** [2]

[1]Ph.D Research Scholar, Department of Computer Science, Vellalar College for Women Thindal, Erode.

[1]Assistsnt Professor, Department of Information Technology,Hindusthan College of arts & Science, Coimbatore.

[2]Assistant Professor, Department of Computer Science, Vellalar College for Women Thindal, Erode.

E-mail: saranyaphd6@gmail.com

ABSTRACT

In order to adapt to the emerging modern world, the use of various techniques in the WSN is to make data transmission faster. In WSN, a variety of techniques are employed to sense and communicate the surrounding environment. During the data transmission time, different types of optimization and algorithms are used to avoid packet losses and time delays. In this present Multiple Node-based Particle Swarm Optimization (MNPSO) algorithm, the optimal rendezvous points are selected, and the energy consumption and packet loss rate are also reduced. The MNPSO algorithm is used to determine the area where the cluster head node is located and how to reduce the delay of data transmission between sources and destinations. Then the shortest path routing is ensured by using the DSR protocol, which is used for fast data collection during data communication for WSN. DSR discovers the best path between SNs, and it denotes the node containing the minimum distance and faster packet transmission in WSN. Also, it avoids congestion; hence, packet loss and routing overhead are reduced prominently.

Keywords: Congestion control, Location finding, Energy consumption, Control packets, Data transmission.

I. INTRODUCTION

Wireless sensor networks (WSNs) have attracted widespread attention in recent years. Due to the low cost, small size and self-organization of sensors. WSNs have been adopted in diverse application fields, such as military, crime prevention, environmental monitoring, health care services, vehicular movements, etc. As sensor nodes are supplied by non-rechargeable batteries [1]. The advancement of WSNs consisting of hundreds/thousands of nodes scattered around the field of study for the fulfillment of a particular mission allows a wide diversity of WSN applications [2]. The design of the new wireless sensor node is an extremely difficult task that requires the analysis of various parameters appropriate for the target application. There is a lot of research in the "security" aspect of WSN [3]. During the design of the WSN security mechanism, the following limitations on the sensor nodes must be noted. These are 1. Low battery life, 2. Limited computation capacity, 3. Low bandwidth, 4. Limited memory, 5. Low communication range. Although both layered and cross layer areas have a lot of scopes, many researchers focus on cross-layer security solutions. The cross-layering principle improves the efficiency of the wireless sensor network communication. Cross-layer is a method for the design of the standard protocol with a reference layer architecture altered as per a specific layered architecture that incorporates the Open System Interconnect (OSI) model interfaces among layers, the development of a protocol [4]. Protocol that is so built will have little conditions in other layers for processing information. The OSI model consists of seven-layered architectures, which have the general networking tasks divided into various layers and their priority of service by using the parameters of individual layers. When the protocols are built for each particular layer, they are also implemented in the respective services. The design of this kind prohibits communication directly between neighbouring layers due to procedural calls and procedural responses [5]. Alternatively, it follows the reference architecture and design protocols allowing direct communication between the protocols and sharing variables at the non-adjoining layers. When the layered structure is violated and parameters between the neighbouring layers are passed, the reference architecture is known as the cross-layer model [6]. Just a few problems caused by wireless sensor nodes can be solved with the cross-layering model. With the help of improvements in the network channel from decreasing at the top layers of the OSI system, the primary features of the wireless medium are ineffectively altered by conventional types of cross layer designs. The purpose of the development of the cross-layer protocol is, therefore, to operate according to changes made within the wireless network conditions [7]. The wireless medium creates the latest modular connections, which are used by the wireless sensor network cross-layer model and it may also be used during the further layering process of the OSI design [8]. This existing research method will not, however, detect malicious events that actually occur in various locations.

PSO is a meta-heuristic search algorithm that plays an important role in increasing the life span of the wireless sensor networks. This algorithm obtains faster and cheaper results compared with other methods. Particle swarm optimization (PSO) is influenced by behavior of birds or fish in a group [9]. In WSN, member nodes transmit their sensor data to the corresponding CH by single or multiple hop communication, and the CHs take the responsibility to process the data fusion and forward the data to the sink. The benefit of clustering can be summarized as follows: (1) Data fusion can be conducted in CHs to fuse the data from their members. Therefore, redundant data can be filtered and the transmission burden of CHs is relieved. (2) It simplifies the topology of the network and reduce the control messages because local nodes only need to know its corresponding CH. Meanwhile, it enhances the scalability of the network. (3) Communication bandwidth is conserved because the intraplate communication usually uses a time division multiple access (TDMA) schema [10].

In this research work, discussion of congestion role in the wireless sensor network is studies. And the congestion aware routing mechanism is routed in wireless sensor network. This is attained by introducing the cross-layer design which will support the congestion avoided reliable data transmission. Successful and reliable packet transmission is guaranteed by predicting the location and movement of nodes based on information gathered from the neighbor nodes. Energy consumption of the WSN nodes is conserved by introducing the location and power aware routing protocol. And also control packet reduction is guaranteed by reducing the number of control packets transmitted.

The respite of this research work is structured as follows: In Section 1, Describes the process of WSNs, the study of PSO Algorithm aspects and an approach to fault monitoring to improve network performance. Section 2, Presents a comprehensive analysis of work related to design and WSN fault monitoring. While in section 3, Analysis of the proposed method, routing based on data transmission. In section 4, discuss the results of the simulation and theoretical analysis. Finally in section 5, overall conclusion of the research work is given based on simulation results attained.

II. RELATED WORKS

Amita Yadav [2018] suggested a PSO algorithm is integrated into the LEACH algorithm for enhancing its performance and to find optimum CHs. The cluster head selection is based on the objective function, which comprises the energy dissipation at cluster head. Which includes the energy consumption between sensor nodes and cluster head, data aggregation cost at cluster head and energy consumption between cluster head and base station

Particle Swarm Optimization (PSO) technique for improving network life time. It helps in forming the clusters as well as the Cluster Head (CH) selection. The proposed algorithm is extensively experimented and then the results of this algorithm are compared with the previously proposed algorithms such as LEACH, etc. It is concluded that the PSO based clustering algorithm gives better results. **Gandhimathi et al [8]** developed the technique of cross-layer detection that maximizes the accuracy of detection with cross-layer and mobile agent-based detection in two phases. Attacks in the first stage are detected through correlating cross-layer functions like MAC and network layers. In the second phase, the mobile agent-based technique is used to avoid the attack if it's been detected. The data is transmitted via the mobile device. Three steps are taken for a mobile agent to overcome the security problem. This approach based on mobile agents will reduce the false positive rate and increase energy efficiency compared to the existing approach. A dynamical, high-level cross-layer security mechanism was developed by **Puri et al [9]** in order to identify various attacks and countermeasures without any network resources. The cross-layer architecture of the security layer offers security-related services and information as yet another feature of the system accessible from any other aspect. Through centralizing all security services within a single component, the overall steadiness and maintenance of the system are improved and the future interactions and dependencies are better controlled than the existing ones. A new security system is suggested based on the perception of cross layer design methodology by **Sharma et al [10]**. Reports are also given on existing cross layer security schemes. This new approach definitely gives a new path in security for WSN, though it does not entitlement to be immune to all the security attacks. Three essential WSN application types have been validated for the cross layer security system. The results showed that when the technique proposed was provided with the right information, energy saving was largely achieved.**Alrajeh et al [11]** suggested an energy-harvesting and cross-layer design security routing protocol and it uses a distributed security mechanism based on a cluster. Parameters between different layers are replaced for efficient energy utilization in the cross-layer design. The energy harvesting system is being used to collect and store energy that is used to determine the node state and therefore the routing issues. The results of the simulation show that in many types of scenery and in a hostile attack-prone situation this routing protocol can perform much better. The WSN trustable model, that uses a cross-layer concept (ACKs from the data link layer and TCP layer) for the development of trust-based models for sensor networks that ensure the trust from a source to sink and isolate the malicious node, was proposed by **Rahhal et al. [12]**. The models are scalable and show high performance with a high percentage of malicious nodes, according to the simulation and analysis results. To get a trustworthy and reliable routing solution in the dynamic WSN environment, **Deng et al. [13]** have developed a Trust-Aware Dynamic Routing Framework (TARF). The proposed TARF may not remove the use of conventional cryptographic approaches and the advanced safety solution to the insecure WSN of today acts as a complementary component. **Bhuiyan et al. [14]** provided the WSN repair and guarantee a specific level of fault tolerance known as Fault Tolerance for Structural Health Monitoring (FTSHM). In a distributed way, FTSHM looks for cluster repair points. FTSHM also includes a decentralized computing SHM algorithm in the energy-constrained WSN to make sure the WSN remains linked to SHM in case of failure, thus extending WSN's lifetime under connectivity and data delivery constraints. Here, the benefits of FTSHM are shown by large simulations of a physical structure. **Geetha et al.[15]** proposed a great notion of fault tolerance based on an Active node to usethe Battery Power and I nterference (AFTBI) WSN model to identify defective nodes for the use of the battery power system and interferen ce model. Fault tolerance against low battery power is planned by hand-off mechanism in which the neighboring node with the highest power is selected in the faulty node and all services are moved to the selected neighboring node by the faulty node. The performance evaluation is evaluated by simulating packet delivery ratio, control overhead, memory overhead, and delay in recovery of faults. We evaluated our tests for different performance measures with Fault Detection in Wireless Sensor Networks (FDWSNs) and found that AFTBI outperforms FDWSN results. **Chen et al [16]** suggested two algorithms to estimate Wireless Sensor Network (WSN) faults. The first is an approximation algorithm for ln(kn), where n is the number of nodes of the sensor. The second is a basic heuristic scheme in which running time is much shorter. In order to analyze our algorithms, we use detailed simulation. The above two algorithms produce results similar to the ILP's optimal solution for relatively dense networks in small networks. The performance of these two algorithms is close to a lower bound for relatively dense networks. A new fault management mechanism to work with fault detection and recovery has been suggested by **Asim et al. [17].** A hierarchical structure is also proposed which allows the proper distribution of fault management tasks between sensor nodes through the introduction of 'self-managing' functions. In comparison with some existing works, the proposed failure detection and recovery algorithm have proved very efficient in energy. The LPS-FMP (Low Power the Speed-the Fault Management Protocol), that is able to promptly respond in cases of abnormal failure, has been proposed by **Liu et al. [18].** The LPS-FMP protocol is primarily intended for Management and Agent two management entities. To achieve a WSN fault management service, it must be ensured that a connection between the management application nodes is created on the Network, which varies from the one specified in the protocol of WSN. The findings suggest that this protocol can detect failures compared to traditional protocols, respond to failures quickly and recover from failures at low cost, increasing the network impact from failure. The Zone-Based Fault Tolerant Management Architecture (ZFTMA), suggested by **Khan et al.[19]**, for WSNs. Two new ideas made up the proposed architecture: a self-organization scheme for energy-efficient networks and a fault management architectural design that provides effective fault detection and recovery mechanisms to endure the fault of the network. This suggested the architecture of ZFTMA can be used to design WSN protocols and applications that show Discussion and Analysis.

III. CONGESTION AWARE ROUTING IN WSN

In this work congestion avoidance is performed by introducing the adaptive congestion window size adjustment procedure. Here the window size for packet transmission will be adjusted by adapting the Support vector machine procedure. Weight based ranking method is introduced for the optimal cross layer design which will support the congestion avoided reliable data transmission. Successful and reliable packet transmission is guaranteed by predicting the location and movement of nodes based on information gathered from the neighbour nodes. Energy consumption of the sensor nodes is conserved by introducing the location and power aware routing protocol. And also control packet reduction is guaranteed by reducing the number of control packets transmitted.

3.3. LOCATION AND POWER AWARE ROUTING

In this location power aware routing is done using MultipleNode based Particle Swarm Optimization method (MNPSO). The MNPSO is a computational approach that optimizes a problem in continuous, multidimensional search spaces. PSO starts with a swarm of random particles. Each particle is associated with a velocity. Particles' velocities are adjusted in order to the historical behaviour of each particle and its neighbours during they fly through the search space. Thus, the particles have a tendency to move towards the better search space. In this work, following factors are considered for the optimal route path selection. Those are Location, power and congestion. Location and congestion are estimated based on equations described in previous sections. The version of the utilized PSO algorithm is described mathematically by the following equations: Each particle updates its own position and velocity in every iteration.

$$v_{id}^{k+1} = \omega \mathrm{v}_{id}^{k} + c_1 \gamma_{1_1}\left(p_{id}^{k} - x_{id}^{k}\right) + c_2 \gamma_{1_2}\left(p_{gd}^{k} - x_{id}^{k}\right) + \alpha(\mathrm{rand} - \frac{1}{2})$$

$$\mathrm{x}_{\mathrm{id}}^{\mathrm{k+1}} = \begin{cases} 1 & \mathrm{s}\left(\mathrm{v}_{\mathrm{id}}^{\mathrm{k+1}}\right) > rand\ (0,1) \\ \quad 0 & \mathrm{else} \end{cases}$$

where the $\mathrm{s}\left(\mathrm{v}_{\mathrm{id}}^{\mathrm{k+1}}\right)$is the sigmoid function S(vid) = 1/(1 + exp(−v_{id})),i = 1, 2, 3 ... m, m is the number of particles in the swarm, $\mathrm{v}_{\mathrm{id}}^{\mathrm{k}}$ and $\mathrm{x}_{\mathrm{id}}^{\mathrm{k}}$stand for the velocity and position of the ith particle of the kth iteration, respectively. $\mathrm{p}_{\mathrm{id}}^{\mathrm{k}}$denotes the previously best position of particle i, $\mathrm{p}_{\mathrm{gd}}^{\mathrm{k}}$ denotes the global best position of the swarm. ω is the inertia weight, c1 and c2 are acceleration constants (the general value of c1 and c2 are in the interval [0 2]), γ1 and γ2 are random numbers in the range [0 1].

Each feature subset can be considered as a point in feature space. The optimal point is the subset with least length and highest classification accuracy. The initial swarm is distributed randomly over the search space, each particle takes one position. The goal of particles is to fly to the best position. By passing the time, their position is changed by communicating with each other, and they search around the local best and global best position. Finally, they should converge on good, possibly optimal, positions since they have exploration ability that equip them to perform FS and discover optimal subsets.

The velocity of each particle is displayed as a positive integer; particle velocities are bounded to a maximum velocity Vmax. It shows how many of features should be changed to be same as the global best point, in other words, the velocity of the particle moving toward the best position. The number of different features (bits) between two particles related to the difference between their positions.

After updating the velocity, a particle's position will be updated by the new velocity. Suppose that the new velocity is V. In this case, V bits of the particle are randomly changed, different from that of Pg. The particles then fly toward the global best while still exploring the search area, instead of simply being same as Pg. The Vmax is used as a constraint to control the global exploration ability of particles. A larger Vmax provides global exploration, while a smaller Vmax increases local exploitation. When Vmax is low, particles have difficulty getting out from locally optimal sections. If Vmax is too high, swarm might fly past good solutions. Objective function is computed as follows

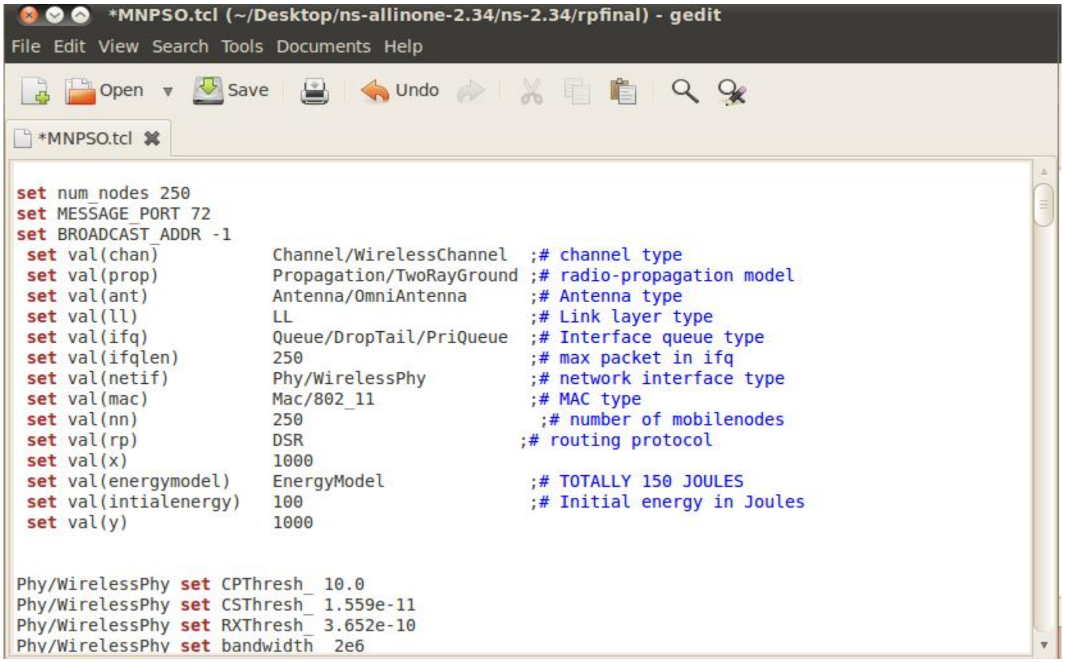
$$(X_i)=\phi.\gamma\left(S^i\right)(t) + \phi(n - |S^i(t)|$$

Where S^i (t) is the feature subset found by particle i at iteration t, and $|S^i$ (t)|is its length. Fitness is computed in order to both the measure of the classifier performance,$\gamma(Si(t))$, and feature subset length. ϕ and φ are two parameters that control the relative weight of classifier performance and feature subset length, ϕ∈[0,1] and φ = 1 − ϕ. It is used to provide optimal CH node by generating the best fitness values of lower energy consumption, lower end to end delay and higher packet delivery ratio.

The above algorithm describes that the N number of sensor nodes are taken for the given network. The objective function is considered as higher packet delivery ratio, lower energy consumption and lower end to end delay metrics. By using MNPSO technique, the path distance is selected which has the capability of defined multi objective function. This algorithm generates better fitness function values and it selects the path which satisfies the threshold values. The MNPSO position is optimized by using best particle and position as well as velocity values. Thus, the MNPSO provides optimal routing path to improve the packet transmission in the larger network. The algorithm describes that the particles in the swarm follow a guiding particle to move to better positions in the search space. The set of all these Pareto-optimal solutions in *X* is called the Pareto-optimal set. It is used to provide reliable and secured path routing for the given network.

IV. RESULTS AND DISCUSSION

The proposed scheme is simulated with Network Simulator tool (NS 2.34). In our simulation, 250sensor nodes move in a 1000-meter x 1000-meter square region, shown in Figure 4 for 60 seconds simulation time. Each node moves independently with the same average speed and the nodes have the same transmission range of 800 meters. The simulated traffic is Constant Bit Rate (CBR).


*MNPSO.tcl (~/Desktop/ns-allinone-2.34/ns-2.34/rpfinal) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
*MNPSO.tcl

```
set num_nodes 250
set MESSAGE_PORT 72
set BROADCAST_ADDR -1
 set val(chan)           Channel/WirelessChannel  ;# channel type
 set val(prop)           Propagation/TwoRayGround ;# radio-propagation model
 set val(ant)            Antenna/OmniAntenna      ;# Antenna type
 set val(ll)             LL                       ;# Link layer type
 set val(ifq)            Queue/DropTail/PriQueue  ;# Interface queue type
 set val(ifqlen)         250                      ;# max packet in ifq
 set val(netif)          Phy/WirelessPhy          ;# network interface type
 set val(mac)            Mac/802_11               ;# MAC type
 set val(nn)             250                       ;# number of mobilenodes
 set val(rp)             DSR                     ;# routing protocol
 set val(x)              1000
 set val(energymodel)    EnergyModel              ;# TOTALLY 150 JOULES
 set val(intialenergy)   100                      ;# Initial energy in Joules
 set val(y)              1000


Phy/WirelessPhy set CPThresh_ 10.0
Phy/WirelessPhy set CSThresh_ 1.559e-11
Phy/WirelessPhy set RXThresh_ 3.652e-10
Phy/WirelessPhy set bandwidth_ 2e6
```

Figure 1: Deployment of Real field sensor nodes over the area of 1000 x 1000m, links are shown in blue line and black dot is the sensor node

Table 1. Simulation settings and parameters

No. of Nodes	250
Area Size	1000×1000
Mac	802.11

Radio Range	800m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512bytes
Mobility Model	Random Walk
Protocol	DSR

A. End to end delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination generally because of queuing and retransmission due to collision.

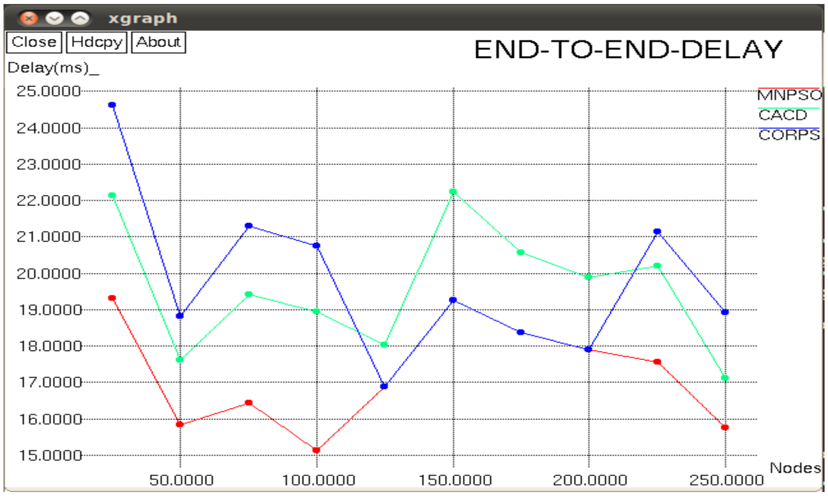


Figure 2. End to End delay comparison

From the above figure we can observe that the comparison of existing and proposed system in terms of end-to-end delay metric. In x axis we plot the number of nodes and in y axis we plot the end-to-end values. In existing scenario, the end-to-end delay values are higher by using MNPSO method. In proposed system, the end-to-end delay value is reduced significantly by using the CORPSP and CADA method. Thus it shows that efficient detection is performed by using proposed method. From the result, we conclude that proposed system is superior in performance.

B. Network lifetime

Lifetime is the time a network operates until the first sensor node or the group of nodes in the network runs out of energy. It can be simply defined as the overall network lifetime that is determined by the remaining energy in the network.

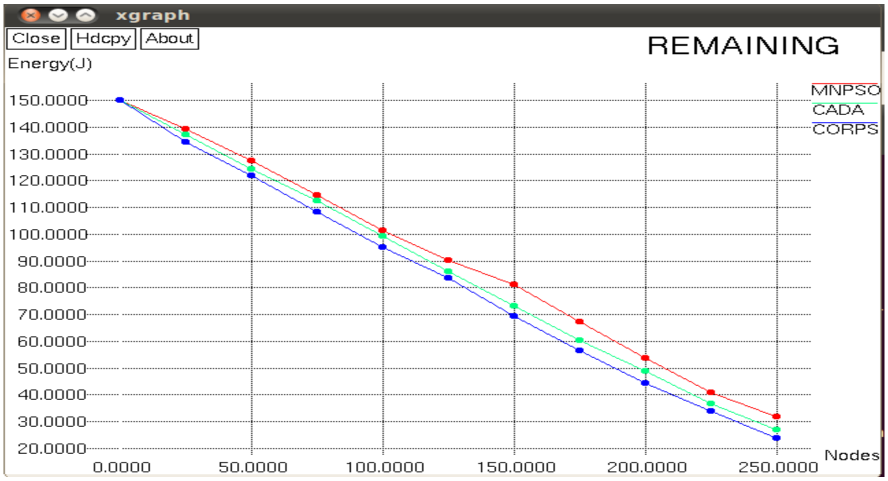


Figure 3. Network Lifetime comparison

From the above figure we can observe that the comparison of existing and proposed system in terms of network lifetime metric. In x axis we plot the number of nodes and in y axis we plot the network lifetime values. In existing scenario, the network lifetime values are lower by using MNPSO method. In proposed system, the network lifetime value is increased significantly by using the CORPSP and CADA method. Thus it shows that efficient detection is performed by using proposed method. From the result, we conclude that proposed system is superior in performance.

C. Throughput

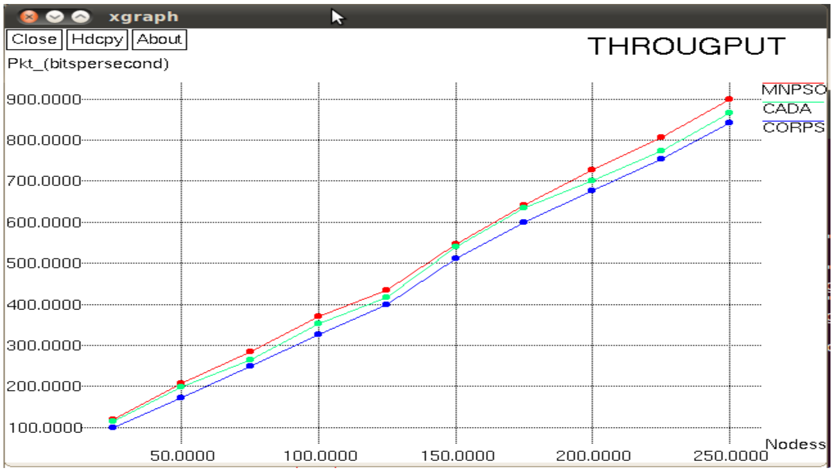


Figure 4. Throughput comparison

Network throughput is described as the typical ratio of successful packet delivery over a message channel. The throughput is usually measured in bits per second (bit/s or bps) and the network is called better when it has high throughput.

From the above figure we can observe that the comparison of existing and proposed system in terms of throughput metric. In x axis we plot the number of nodes and in y axis we plot the throughput values. In existing scenario, the throughput values are lower by using MNPSO method. In proposed system, the throughput value is increased significantly by using the CORPSP and CADA method. Thus it shows that efficient detection is performed by using proposed method. From the result, we conclude that proposed system is superior in performance.

D. Packet delivery ratio

Packet delivery ratio is defined as the number of packets successfully received by the destination.

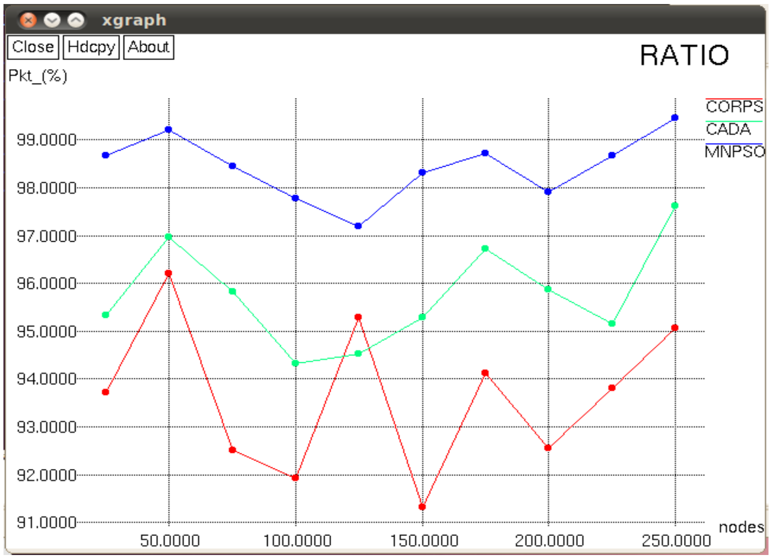


Figure 5. Packet delivery ratio comparison

From the above figure we can observe that the comparison of existing and proposed system in terms of packet delivery ratio. In x axis we plot the number of nodes and in y axis we plot the packet delivery ratio values. In existing scenario, the packet delivery ratio values are lower by using MNPSO method. In proposed system, the packet delivery ratio value is increased significantly by using the CORPSPand CADA method. Thus it shows that efficient detection is performed by using proposed method. From the result, we conclude that proposed system is superior in performance.

V. CONCLUSION

Successful and reliable packet transmission is guaranteed by predicting the location and movement of nodes based on information gathered from the neighbour nodes. Energy consumption of the sensor nodes is conserved by introducing the location and power aware routing protocol. And also control packet reduction is guaranteed by reducing the number of control packets transmitted. The overall analysis of the research work is done in the NS2 simulation environment from which it is proved that the proposed method attains better outcome.

REFERENCE

1. Danwei Ruan and Jianhua Huang "A PSO-Based Uneven Dynamic Clustering Multi-Hop Routing Protocol for Wireless Sensor Networks" pp(1-24), Sensors 2019. doi:10.3390/s19081835.
2. Anita, X., Bhagyaveni, M. A., &Manickam, J. (2014). Fuzzy-based trust prediction model for routing in WSNs. *The Scientific World Journal*, *2014*.
3. Su, W., & Lim, T. L. (2006, June). Cross-layer design and optimization forwireless sensor networks. In *Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'06)* (pp. 278-284). IEEE.
4. Liu, S., Bai, Y., Sha, M., Deng, Q., & Qian, D. (2008, October). CLEEP: A novel cross-layer energy-efficient protocol for wireless sensor networks. In *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-4). IEEE.
5. Khan, S., Loo, K. K., & Din, Z. U. (2009). Cross layer design for routing and security in multi-hop wireless networks. *Journal of information assurance and security*, *4*(2), 170-173.
6. Rajaram, A., &Palaniswami, D. S. (2009). A trust based cross layer security protocol for m-obile ad hoc networks. *arXiv preprint arXiv:0911.0503*.
7. Sharma, K., &Ghose, M. K. (2011). Cross layer security framework for wireless sensor networks. *International Journal of Security and Its Applications*, *5*(1), 39-52.
8. Gawdan, I. S., Chow, C. O., Zia, T., &Gawdan, Q. I. (2011). Cross-layer based security solutions for wireless sensor networks. *International Journal of Physical Sciences*, *6*(17), 4245-4254.
9. Amita Yadav1, Suresh Kumar2, 3 Singh Vijendra " Network Life Time Analysis of WSNs Using Particle Swarm Optimization " International Conference on Computational Intelligence and Data Science (ICCIDS 2018) ,pp(805–815), Elsevier-2018.
10. Jin Wang, Yu Gao , Wei Liu , Arun Kumar Sangaiah and Hye-Jin Kim "An Improved Routing Schema with SpecialClustering Using PSO Algorithm for Hetero generous Wireless Sensor Network" Sensor, pp(1-17),2019, doi:10.3390/s19030671.
11. Gandhimathi, L., &Murugaboopathi, G. (2016, February). Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent. In *2016 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 1-5). IEEE.
12. Puri, S., &Tripathi, S. P. (2012). Dynamic high level cross layer security mechanisms for wireless sensor networks. *International Journal of Information Technology and Computer Science (IJITCS)*, *4*(6), 45-56.
13. Sharma, K., &Ghose, M. K. (2011). Cross layer security framework for wireless sensor networks. *International Journal of Security and Its Applications*, *5*(1), 39-52.
14. Alrajeh, N. A., Khan, S., Lloret, J., & Loo, J. (2013). Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *9*(1), 374796.
15. Rahhal, H. A., Ali, I. A., &Shaheen, S. I. (2011, April). A novel trust-based cross-layer model for wireless sensor networks. In *2011 28th National Radio Science Conference (NRSC)* (pp. 1-10). IEEE.
16. Deng, H., Yang, Y., Jin, G., Xu, R., & Shi, W. (2010, December). Building a trust-aware dynamic routing solution for wireless sensor networks. In *2010 IEEE Globecom Workshops* (pp. 153-157). IEEE.
17. Bhuiyan, M. Z. A., Wang, G., Cao, J., & Wu, J. (2013). Deploying wireless sensor networks with fault-tolerance for structural health monitoring. *IEEE Transactions on Computers*, *64*(2), 382-395.
18. Geeta, D. D., Nalini, N., &Biradar, R. C. (2013). Fault tolerance in wireless sensor network using hand-off and dynamic power adjustment approach. *Journal of Network and Computer Applications*, *36*(4), 1174-1185.
19. Chen, X., Kim, Y. A., Wang, B., Wei, W., Shi, Z. J., & Song, Y. (2012). Fault-tolerant monitor placement for out-of-band wireless sensor network monitoring. *Ad Hoc Networks*, *10*(1), 62-74.
20. Asim, M., Mokhtar, H., &Merabti, M. (2010). A self-managing fault management mechanism for wireless sensor networks. *arXiv preprint arXiv:1011.5072*.
21. Liu, T. H., Yi, S. C., & Wang, X. W. (2013). A fault management protocol for low-energy and efficient wireless sensor networks. *J. Inf. Hiding Multimedia Signal Process*, *4*(1), 34-45.
22. Khan, M. Z., Merabti, M., Askwith, B., &Bouhafs, F. (2010, June). A fault-tolerant network management architecture for wireless sensor networks. In *11th Annual PGNet 2010 Conference, At Liverpool John Moores University, UK*.