ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SEEDAL: SECURE, ENERGY-EFFICIENT, DELAY-AWARE, AND LIFETIME-BALANCING ROUTING PROTOCOL FOR HETEROGENEOUS WIRELESS SENSOR NETWORKS

Ms. Arya R*, Dr. N. K. Sakthivel

* M.Tech Student Department of Computer Science and Engineering Nehru College of Engineering and Research Centre Thrissur, Kerala, India

Member , IEEE Vice Principal Nehru College of Engineering and Research Centre Thrissur, Kerala, India

DOI:

ABSTRACT

The latest research on Open Vehicle Routing (OVR) problems, a dynamic territory in operational research depends upon some features and requirements which can be contrasted with requirements in Wireless Sensor Networks domain. According to this perception, the computational overheads in Open Vehicle Routing can be compared to Routing problems in Wireless Sensor Network. To show that this methodology is possible, one data collection protocol called EDAL, was developed. The conservation of credibility and protection of the data is not considered in the outline of the EDAL protocol. Keeping in mind the end goal to conquer the issue with respect to the secure data transmission in EDAL, another protocol called SEEDAL, which remains for Secure, Energy-Efficient, Delay-Aware, and Lifetime-Balancing Routing Protocol for Heterogeneous Wireless Sensor Networks (SEEDAL) which provides a secure routing mechanism considering the concept of secret key sharing by means of encryption and decryption during the data transmission and data reception It likewise considers expense of giving security and some of its major impact on energy effectiveness. The design of SEEDAL protocol is efficient in terms of packet delay, network lifetime, energy efficiency, energy consumption.

KEYWORDS: Secure Data Transmission, SEEDAL, EDAL, Clustering, Data Aggregation.

INTRODUCTION

WSN comprise of spatially disseminated self-sufficient sensors to monitor physical or ecological conditions, for example, temperature, sound to agreeably pass data to principle location. It is comprised of radio transmitter, microcontroller and sensor nodes. As of late, remote sensor systems (WSNs) have risen as another classification of systems administration frameworks with restricted processing, correspondence, and capacity assets. A WSN is utilized for an extensive variety of uses, for example, environment monitoring, scientific perception, crisis location, field reconnaissance, and structure monitoring. In the specimen applications, drawing out the lifetime of WSN and ensuring packet delivery delays are basic for accomplishing worthy nature of administration. WSNs utilize multi-hop directing to execute data gathering. Every sensor node assumes the part of data authority and in addition message forwarder in the system. Data transmission and data gathering in a Wireless Sensor Network needs a directing convention which utilizes legitimate data aggregation methods. The regular need of numerous detecting applications is an efficient directing convention which ought to guarantee that their source nodes convey packets to sink node through different hops in required time spans. Features of an efficient Routing Protocol are listed below:

Minimum Energy Consumption: The nodes and sensors present in the WSN ought to devour minimum measure of energy. This can be accomplished by bringing down the energy cost in transmitting the parcels.

Maximum Energy Efficiency: Since nodes included in WSN are for the most part battery controlled gadgets, the outline objective of the steering convention is to streamline the measure of energy use for transmission.

Minimum Delay: The bundles must be conveyed to the destination inside of certain time limit. Generally there is chance for the event of postponement. In this way the directing convention is to be outlined in a manner that correspondence inertness ought to be minimized.

Maximum Lifetime: Time taken by node to drain its energy is called as lifetime of that node. The time until first node in WSN die is called as lifetime of network. A decent steering convention ought to amplify lifetime of the nodes and system.

Lately, Wireless Sensor Networks (WSNs) have developed as another class of systems administration frameworks with restricted computing, correspondence, and capacity assets. A WSN comprises of nodes conveyed to sense physical or ecological conditions. Numerous detecting applications [1] offer in like manner that their source nodes convey packets to sink nodes by means of different hops, prompting the issue on the best way to find courses that empower all packets to be conveyed in required time allotments, while at the same time considering variables, for example, energy efficiency and burden adjusting. Numerous past examination endeavors have attempted to accomplish tradeoffs as far as deferral, vitality cost, and load-adjusting for such information gathering assignments. Our key inspiration for this work originates from the knowledge that late research endeavors on open vehicle routing (OVR) issues are typically in view of comparative presumptions and constraints contrasted with sensor networks. Specifically, in OVR research on goods transportation, the goal is to spread the products to clients in finite time with the negligible measure of transportation expense. One may ponder actually, on the off chance that we regard packet delays as conveyance time of products, and energy cost as conveyance expense of good, it might be conceivable to adventure exploration results in one domain to simulate other.Fig. 1 shows a sample Wireless Sensor Network

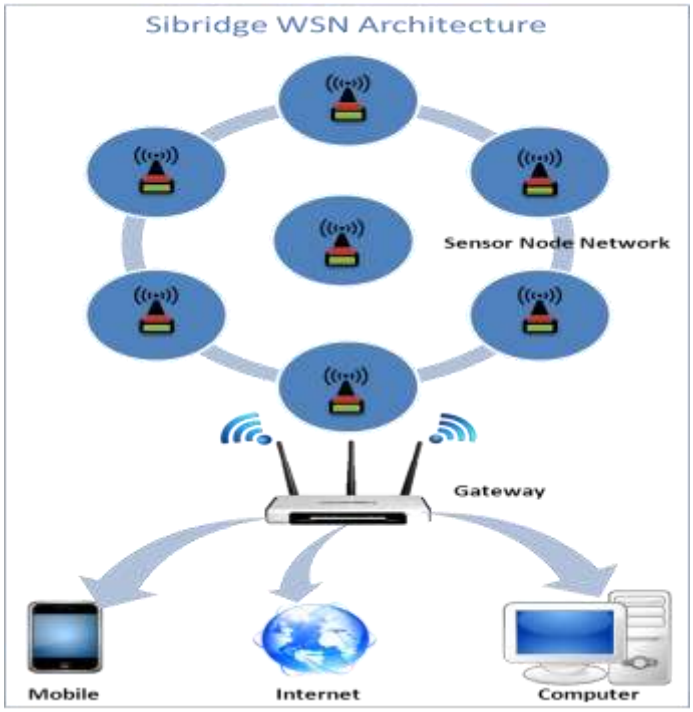

Fig. 1: Sample Wireless Sensor Network

RELATED WORKS

Wisden, a Wireless Sensor Network System for structural response data acquisition[7] continuously collects structural response data from a multi-hop network of sensor nodes, and displays and stores the data at a base station The system mimics wired data acquisition systems, and incorporates novel reliable transport, time synchronization, and compression algorithms .But it is failed to gain significant experience with the systems overall accuracy and performance by deploying it on several large structures at different scales.

ISSN: 2277-9655
Impact Factor: 3.785

Another protocol called EDAL which stands for Energy-Efficient ,Delay-Aware, Lifetime-Balanced Routing Protocol for Heterogeneous Wireless Sensor Networks[1] employees centralized meta-heuristic employs tabu search to find approximate solutions and assume that nodes have been selected as sources at the beginning of each data collection period. The heuristic algorithm (Centralized-EDAL) consists of two phases namely route construction and route optimization .

One problem with the centralized heuristic algorithm it requires information to be collected from each node to a centralized one. In distributed sensor networks, this step will typically incur additional overhead. It is usually desirable to distribute the algorithm computation into individual nodes.

Distributed heuristics algorithm for EDAL(D-EDAL), where at the beginning of each period, each source node independently chooses the most energy-efficient route to forward packets based on ant colony based gossiping algorithm.

In existing routing protocols such as EDAL, C-EDAL and D-EDAL some of the important constraints which are adequate for a wireless sensor network are not satisfied like protocol needs to serve tighter minimum delay requirements. In that case, each route will consist of fewer source nodes. Security in data transmission is not achieved in the existing routing protocols .In distributed heuristics, energy efficiency is low and in centralized heuristics, battery life of base station node needs to be considered .In order to overcome this problems, a new protocol called SEEDAL which stands for Secure, Energy-Efficient, Delay-Aware and Lifetime-Balanced Routing Protocol for Heterogeneous Wireless Sensor Networks is developed.

SEEDAL

Effective data transmission is a standout amongst the most vital issues for WSNs. In the interim, numerous WSNs are sent in harsh, neglected, and frequently adversarial physical situations for specific applications, for example, military spaces and detecting assignments with trustless surroundings. Secure and efficient data transmission (SET) is, hence, particularly important and is requested in numerous such functional WSNs. Cluster based information transmission in WSNs has been explored by scientists to accomplish the system adaptability and administration, which boosts hub lifetime and decrease data transfer capacity utilization by utilizing nearby joint effort among sensor hubs. In a Cluster based WSN (CWSN), each cluster has a pioneer sensor node, viewed as cluster head (CH).

A CH totals the information gathered by the leaf nodes (non-CH sensor nodes) in its group, and sends the conglomeration to the base station (BS). The low-vitality versatile clustering chain of importance (LEACH) convention exhibited is a generally known and successful one to lessen and adjust the aggregate energy utilization for CWSNs.

To anticipate speedy energy utilization of the arrangement of CHs, LEACH arbitrarily pivots CHs among all sensor nodes in the system, in rounds. On the other hand, the cluster's execution based construction modeling in this present reality is fairly confused. Adding security to LEACH-like conventions is testing on the grounds that they progressively, haphazardly, and occasionally revise the system's groups and information joins.

NETWORK ARCHITECTURE

Consider a CWSN comprising of an altered Base Station (BS) and large number of sensor nodes (SN), which are homogeneous in functionalities and capabilities. We expect that the BS is constantly dependable, i.e., the BS is a trusted authority (TA). Then, the sensor nodes may be traded off by aggressors, and the data transmission may be hindered from assaults on remote channel. In a CWSN, sensor nodes are gathered into clusters, and every cluster has a CH sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes join a cluster contingent upon the getting signal quality and transmit the detected data to the BS by means of CHs to spare vitality. The CHs perform data combination, and transmit data to the BS straightforwardly with relatively high vitality.

Moreover, we acknowledge that all sensor nodes and the BS are time synchronized with symmetric radio channels and nodes are disseminated arbitrarily with their energy distributed. In CWSNs, data detecting, preparing, and

transmission devour energy of sensor nodes. The expense of data transmission is much more expensive than that of data preparing. In this manner, the strategy that the intermediate node (e.g., a CH) totals data and sends it to the BS is favored than the system that every sensor node specifically sends data to the BS. A sensor hub switches into rest mode for energy sparing when it doesn't sense or transmit data, contingent upon the time-division different access (TDMA) control utilized for data transmission.

SECURITY VULNERABILITIES AND PROTOCOL OBJECTIVES

The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are defenseless against various security attacks. Particularly, attacks to CHs in CWSNs could bring about genuine harm to the network on the grounds that data transmission and data aggregation rely on upon the CHs on a very basic level. On the off chance that an attackers figures out how to trade off or put on a show to be a CH, it can incite attacks, for example, sinkhole and particular sending attacks, thus upsetting the network. Then again, an attacker may expect to infuse sham detecting data into the WSN, for instance, imagine as a leaf node sending false data toward the CHs. By the by, LEACH-like protocols are more strong against insider attacks than different sorts of protocols in WSNs. It is on account of CHs are pivoting from nodes to nodes in the network by rounds, which makes it harder for gatecrashers to distinguish the steering components as the mediator nodes and assault them. The qualities of LEACH-like protocols diminish the dangers of being assaulted on middle person nodes, and make it harder for a foe to distinguish and trade off critical nodes (i.e., CH nodes).

The objective of SEEDAL is secure data transmission for CWSNs is to ensure the protected and effective data transmissions between leaf nodes and CHs, and in addition transmission in the middle of CHs and the BS. In the interim, the vast majority of existing secure transmission conventions for CWSNs in the writing, on the other hand, apply the symmetric key management for security, which experiences the orphan node issue. SEEDAL means to take care of this orphan node issue by utilizing the ID based cryptosystem that ensures security necessities. Fig. 2 demonstrates the working of SEEDAL convention.

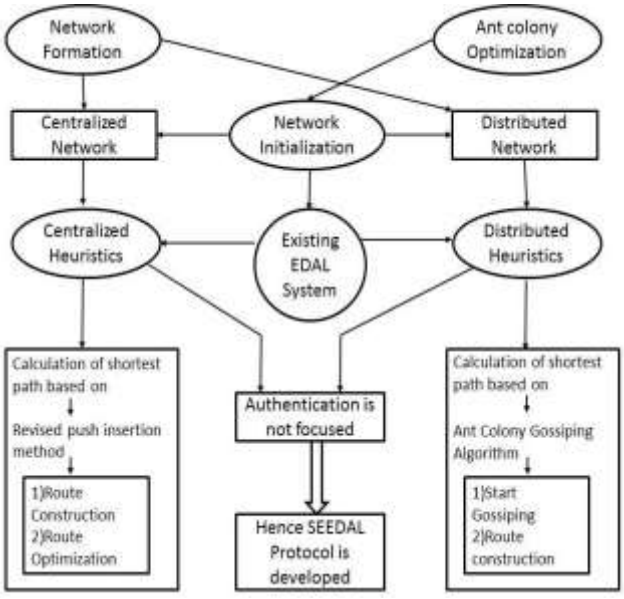

Fig. 2: SEEDAL Protocol

In order to ensure security the accompanying methodology is utilized by SEEDAL. SEEDAL actualized for CWSNs comprises of the accompanying operations, particularly, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data accepting nodes:

(i) Setup: The BS (as a trust authority) produces an expert key msk and public parameters param for the private key generator (PKG), and offers them to all sensor nodes.

ISSN: 2277-9655
Impact Factor: 3.785

(ii) Extraction: Given an ID string, a sensor node produces a private key sekID connected with the ID utilizing msk.

(iii) Signature signing: Given a message M, time stamp t and a signing key, the sending node produces a signature SIG.

(iv) Verification: Given the ID, M, and SIG, the getting hub yields "accept" if SIG is legitimate, and yields "reject" generally.

The cluster which takes after the centralized heuristics goes about as a fixed base station. A node in the base station is in charge of producing a master key, parameter and private key generators (PKG) for every other node. Just a trusted authority can create a master key, parameter and PKGs. With a given id the sensor node makes its own particular signature. The sending hub appoints timestamps to the messages and produces the message id (MID). At that point those messages are transmitted. At the point when the transmitted messages achieve the destination, the receiver checks the MID. The message is accepted on the off chance that it is "accept" or it is rejected.

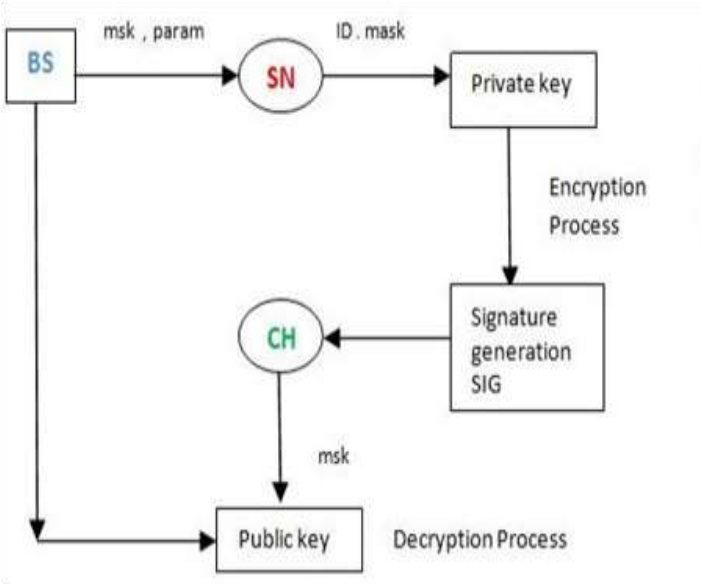

Fig. 3. Security mechanism-SEEDAL

SEEDAL relies on ID based cryptography in which user public keys are their ID data. Thus, clients can acquire their relating private keys without auxiliary information transmission, which is effective in communication and saves energy. Fig. 3 illustrates the process of encryption and decryption utilizing the keys produced. As appeared in Fig.3private key is generated from nodes ID and the mask (msk) function of Base station (BS). Similarly, public key is generated from msk function of CH. Using these keys security can be provided to the data.

The SEEDAL protocol is tested using the Network Simulator. Start of network initialization of SEEDAL using 61 nodes in a sparse network and their movement within the network is simulated using NS2.

In sparse network the nodes were distributed over a wide area (not dense) where a multihop situation is obtained. Also the nodes were deployed in such a way that the scenario has a traffic flow close to real condition .It is important to have an idea while forming the cluster that the minimum separation distance affects the energy consumption ,i.e. the number of messages received at the base station during the lifetime of the network and how the number of clusters used affects the energy consumption in the network.

ISSN: 2277-9655
Impact Factor: 3.785

PERFORMANCE EVALUATION

To evaluate the performance of SEEDAL, the simulation consisting of 61 heterogeneous nodes scattered randomly was considered and the following graphs were obtained while considering different parameters like throughput, minimum delay, maximum energy efficiency, routing overhead and packet loss.

Fig. 4shows the network throughput analysis for Routing Protocols namely SEEDAL and C-EDAL. Red colour in the graph indicates network throughput of C-EDAL protocol whereas the green color indicates the network throughput of SEEDAL protocol..

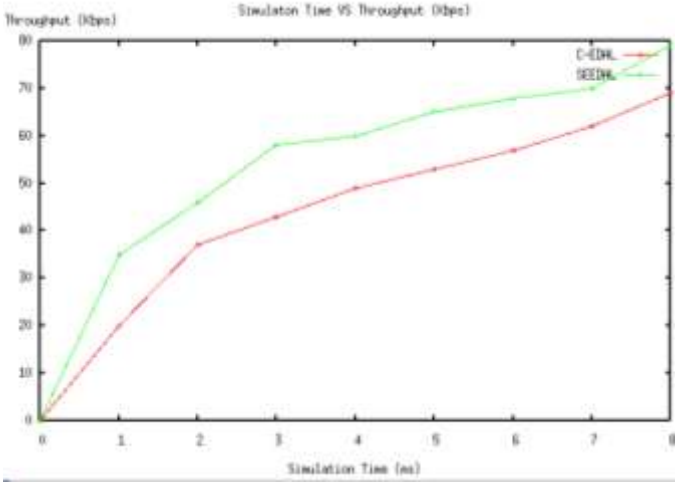

Fig. 4. Network Throughput Analysis for SEEDAL and C-EDAL

Average Energy Consumption of the network running different algorithm according to the simulation time is illustrated in Fig. 5 SEEDAL is represented by green colour. Red colour in the graph indicates energy consumption while using C-EDAL protocol

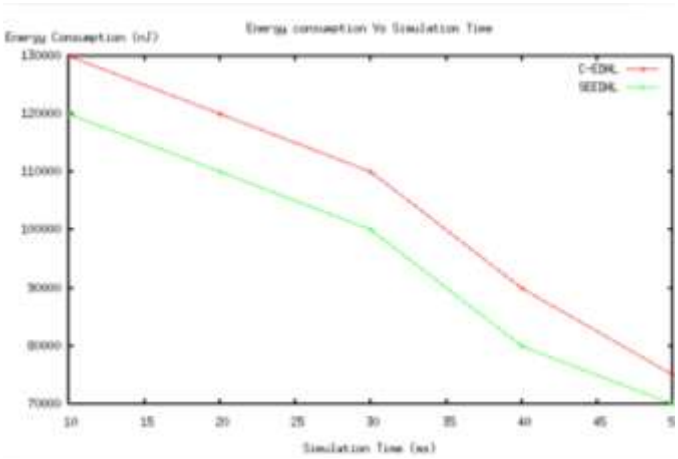

Fig. 5. Average Energy Consumption of the network running SEEDAL and C-EDAL

ISSN: 2277-9655
Impact Factor: 3.785

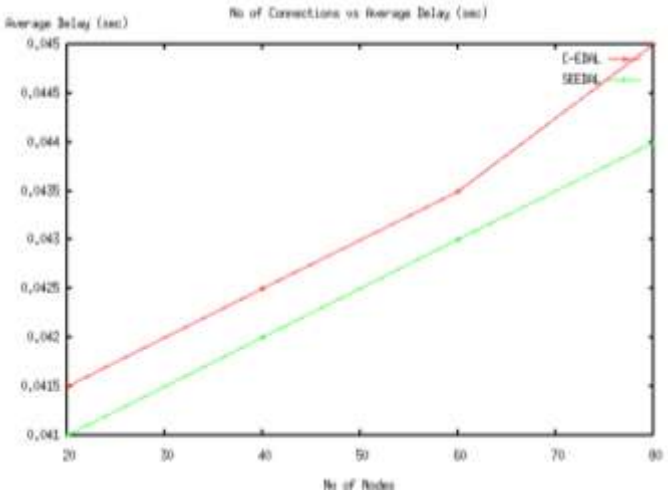

Fig. 6. Comparison of Delay between SEEDAL and existing protocol

Comparison of Average Delay between SEEDAL and existing protocol is illustrated in Fig 6..Red color in the graph indicates C-EDAL and green color represents SEEDAL .It is clear that the delay is minimum in case of SEEDAL comparing with the C-EDAL protocol

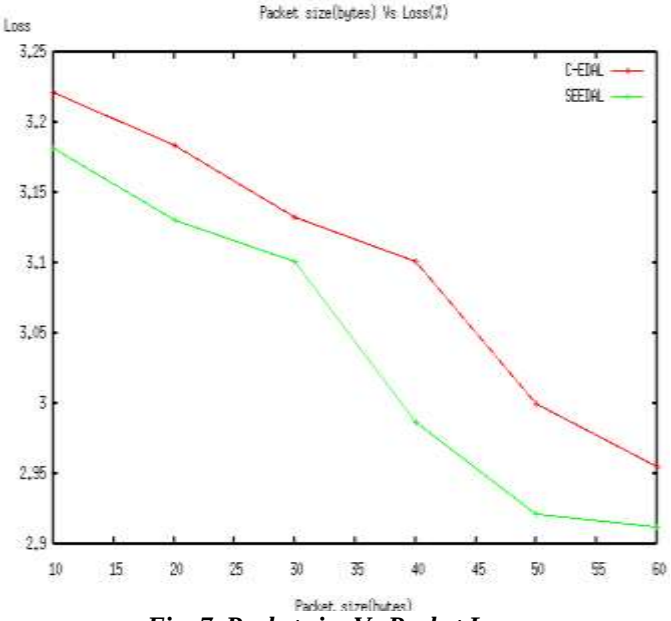

Fig. 7. Packet size Vs Packet Loss

Fig.7 shows the dependency between size of the packet and packet loss. As the size of the packet increases, the packet loss is minimum in the case of SEEDAL compared to C-EDAL.

So there exist an inverse relationship between the size of the packet and loss of the packet

ISSN: 2277-9655
Impact Factor: 3.785

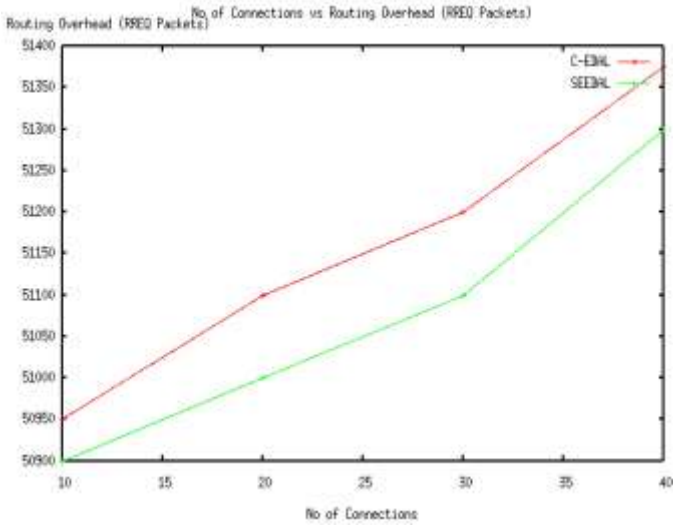

Fig. 8.Routing overhead in SEEDAL and EDAL

Fig. 8 shows the routing overhead in Routing Protocols according to the number of connections. From the graph it is clear that SEEDAL outperforms C-EDAL when routing overhead is considered.

CONCLUSION

SEEDAL is designed as an energy efficient routing schema which ensures security during data transmission in Wireless Sensor Networks. In past researches several protocols were designed for energy efficient routing in WSN but effect of security precautions on cost of energy spending during routing was not focused. Considering raise in security threats to WSN route it is now become essential to provide security during routing. However the existing Routing Protocol EDAL, in which the centralized method the parameters like lifetime, energy-efficiency were focused whereas distributed method in which parameters like minimum delay requirement was focused. But the overall security during data transmission is not considered in both these methods. SEEDAL is a secure routing schema considering secret sharing encryption and decryption algorithms. It also considers cost of providing security and its effect of energy. A system study has been given to evaluate the network throughput. Simulation results have been provided to validate the model and to demonstrate the improvement in the performance of the network.

FUTURE SCOPE

The methodology for the development of a generic method for finding the optimal number of clusters in order to maximize the energy efficiency can be considered for future studies regarding Routing Protocols for Wireless Sensor Networks.

REFERENCES

[1] M. I. A. Yanjun Yao, Qing Cao and A. V. Vasilakos, “An Energy Efficient, Delay-Aware, Lifetime-Balancing Routing Protocol for Heterogeneous Wireless Sensor Network,” IEEE Trans. Net, vol. 67, pp. 56–60, 2014.
[2] Q. Ling and Z. Tian, “Decentralized Sparse Signal Recovery for Compressive Sleeping Wireless Sensor Networks,” IEEE Transactions on Signal Processing, vol. 58, pp. 3816– 3827, 2010.
[3] B. L. G. Christopher C. Skiscim, “Optimisation by Simulated Annealing: A Preliminary Computational Study For The TSP,” in Winter Simulation Conference, 1983.
[4] M.Hosny,“Heuristic Techniques for Solving the Vehicle Routing Problem With Time Windows,” in International Conference on Future Informaion Technology, 2011.
[5] S. H. e. a. K. Saleem, N. Fisal, “Ant based Self-Organised Routing Protocol for Wireless Sensor Networks,” International Journal Of Communication Networks and Information Security, pp. 42–46, 2009.

[6] J. L. Liu Xiang and C. Rosenberg, "Compressed Data Aggregation: Energy Efficient and high Fidelity data collection," 2009.
[7] K.K.C.D.G.A.B.R.G.N.Xu,S.Rangwalaand D.Estrin,"Awireless Sensor Network For Structural Monitoring," in Proc. 2nd ACM SenSys, New York, NY, USA, 2004.
[8] X. Z. L. Liu and H. Ma, "Optimal Node Selection For Target Localization In Wireless Camera Sensor Networks," IEEE Trans. Veh.Technol., vol. 59, pp. 44–50, 2011.
[9] D. B. C. Caione and L. Benini, "Distributed Compressive Sampling For Lifetime Optimization In Dense Wireless Sensor Networks," IEEE Trans. Ind. Inf., vol. 8, pp. 30–40, 2012.