

Extending Security and Lifetime of Wireless Sensor Networks by Implementing Secure Routing Protocol

Jomma Prathap, M.Tech, Dept of CSE, Vishwa Bharathi College Of Engineering, Kukatpally, Hyderabad, Telangana, India. Email: prathapjomma@gmail.com

Matla Himagireswar Rao, M.Tech, Assistant Professor, Dept of CSE, Vidya Jyothi Institute Of Technology, Aziz nagar, Hyderabad, Telangana, India. Email: maatlahima@gmail.com

ABSTRACT— *In current days, remote systems are confronting number of issue to exchange the information from source to goal through the diverse routings. In that two noteworthy issues are exceedingly impact on systems those are arrange lifetime and security. Accordingly, lifetime enhancement and security are the major testing configuration issues in this paper. To accomplish these two difficulties interestingly we proposed Cost Aware Secure Routing (CASER) convention in this paper. Concurring this paper, in existing we utilized uniform vitality organization in the systems. Through this uniform vitality sending procedure, arrange lifetime diminished very. For that in our convention we give non-uniform vitality arrangement methodology. Essentially, our convention works through two customizable parameters which are 1) Energy Balance Control (EBC) 2) Random Walking. Our convention can altogether enhance the system lifetime alongside security.*

1. INTRODUCTION

As of late, Wireless Sensor Networks (WSNs) has been for the most part utilized as a part of utilizations, for example, wellbeing, military, also, natural checking; this development has been powered by its broad fame in remote correspondence. Be that as it may, there are restrictions because of vitality imperatives. Due to the vitality level variety, the arrange lifetime gets decreased. Consequently, impressive exertion is expected to make it more effective. To boost the system lifetime, the vitality utilization of the hub ought to be decreased. As of late, a noteworthy research in this range has been on the utilization of unified and limited k-scope calculations. The proposed calculation states that relying upon the system measure; the system is reconfigured to any of the calculations to limit the vitality wastage. Though, networking and security machineries are in a progressive stage, wireless

sensor networks present convolutions which dictate the scheme of new protocols. First, these grids organize in an infrastructure-less ad hoc manner, which denotes that the interaction relies on the collaboration between nodes for the attainment of basic networking tasks such as routing. Each time a sensor requests to send the recognized value to the data basin, it glances for an available neighbor. As these are ad hoc networks planned to organize in a self-organized fashion, a malicious node may arrive the network. Due to the wireless strategy, snooping can be easily achieved in this environment which creates the network accessible not only to privacy attacks, but also to traffic exploration attacks which threaten the whole grid operation. Cryptography and authentication can assist but do not avail due to the constraints described. To this end, security is extremely vulnerable in wireless sensor networks and the routing system is at the focus of adversaries due to its significance for the suitable network operation

and its vulnerability led by the required collaboration. The up to date interest in sensor networks has headed to a number of routing patterns that use the limited resources available at sensor nodes more efficiently. Routing is the essential design concern for WSN. A well planned routing protocol provides a smaller amount of energy depletion for communication and has the good message delivery ratio. To expand the Sensor network lifetime and also manage entire sensor network energy depletion wireless Sensor Networks has the solution which supports extensive range of applications. Based on the type of application, their WSN environs it is the risky, perplexing and rarer problematic. Even, the programmed Security schemes in WSNs not to observe the node tangible internment, the malicious nodes. So, unique security systems are important for the secure transmission of message from source to sink. A novel system of attaining security in absence of cryptography is defined as Trust based security where Trust is termed as -The sign of Trustworthiness. It collects the nodes information and observes the action of other nodes as well as the details of communication in the grid either directly or indirectly. By using all these information trust value will be calculated. To look after the decision making methods of the network Trust management will be used and it also helps to identify the unsecured nodes. Several observations on trust related with WSN are done, but it is critical to design and develop a trust management scheme which uses the minimum amount of resources of the node and also to maintain the trust among the nodes in the grid. In a Wireless Sensor Network trust management will be as a simple one if it doesn't have the limitations on consumptions of energy, and easy to adopt the changes.

2. RELATED WORK

Alshowkan et al., Have proposed a light-weight Secure-Low-energy Adaptive Clustering Hierarchy (LSLEACH) where they firstly discourage the attacker to become a member of the wireless sensor community utilizing light-weight and vigor-effective authentication operate in which the cluster head verifies the validity of nodes, which ask to join the cluster. Secondly, they described the brink for the natural node-to-node number of connections by means of the time. That is used to become aware of the strange pursuits occurred between nodes. Thirdly, they described the effective use of time division multiple access (TDMA) in the LEACH so that every node can handiest send information to the cluster head. Additionally they described the mechanism to use LS-LEACH in WSNs with the aid of election, connection, and transmission where special formulations are used. They count on that each node has two secret keys. One key's shared among all nodes, and additionally it is shared with the base station. When the node turns into a cluster head, then the confidential key can be shared with the bottom station. Then again, the workforce key's used to become a member of clusters. In addition they expect that the number of cluster heads will have to not be more than 5% of total nodes. The beginning of each subsequent cycle after community deployment, cluster head will be elected. They describe that wireless sensor network is facing lots of problems reminiscent of insufficient resources in power, energy consumption and storage. There's yet another challenge that the individuality of the published medium makes the wireless sensor networks at risk to a number of assaults. An attacker can join the wireless sensor community and may just snatch, insert or broadcast the info. They in comparison the efficiency of LS-LEACH and LEACH making use of

approach throughput, lifetime of the network and the quantity of energy they consumed.

Routing may be a difficult task in WSNs attributable to the restricted resources. Geographic routing has been wide viewed as one of the foremost promising approaches for WSNs. Geographic routing protocols utilize the geographic location information to route knowledge packets hop-by-hop from the source to the destination. The supply chooses the immediate neighboring node to send the message supported either the direction or the gap. The gap between the neighboring nodes is calculable or acquired by signal strengths or mistreatment GPS equipments. The relative location info of neighbor nodes will be changed between neighboring nodes. A Geographic Adaptive Fidelity (GAF) routing scheme was planned for detector networks prepared with low energy GPS receivers. In GAF, the network space is divided into mounted size virtual grids. In every grid, only one node is chosen because the active node, whereas the others will sleep for an amount to save lots of energy. The detector forwards the messages supported greedy geographic routing strategy. A query primarily based Geographic and Energy Aware Routing (GEAR) was planned. In GEAR, the sink node disseminates requests with geographic attributes to the target region rather than mistreatment flooding. Every node forwards messages to its neighboring nodes supported calculable cost and learning value. The calculable value considers each the gap to the destination and also the remaining energy of the detector nodes. Whereas, the educational cost provides the change info to contend with the local minimum drawback; while geographic routing algorithms have the benefits that each node solely must maintain its neighboring information, and provides a better potency and a more robust

scalability for giant scale WSNs, these algorithms might reach their native minimum, which may end in dead finish or loops. To solve the native minimum drawback, some variations of these basic routing algorithms were planned, including GEDIR, MFR and compass routing rule. The delivery magnitude relation is improved if every node is conscious of its two-hop neighbors. There are a couple of papers mentioned combining greedy and face routing to resolve the native minimum drawback. The essential plan is to line the native topology of the network as a flattened graph, and so the relay nodes attempt to forward messages on one or probably a sequence of adjacent faces toward the destination. Lifetime is another space that has been extensively studied in WSNs. A routing theme was planned to find the sub-optimal path that may extend the period of time of the WSNs rather than perpetually choosing all-time low energy path. Within the planned theme, multiple routing methods are ready ahead by a reactive protocol like AODV or directed diffusion. Then, the routing theme can select a path primarily based on a probabilistic technique in keeping with the remaining energy. Yangtze River and Tassiulas assumed that the transmitter energy level is adjusted in keeping with the distance between the transmitter and also the receiver. Routing was developed as an applied mathematics drawback of neighboring node choice to maximize the network period of time. Then Zhang and Shen investigated the unbalanced energy consumption for uniformly deployed data collecting sensor networks. During this paper, the network is divided into multiple corona zones and every node will perform data aggregation. A localized zone-based routing scheme was planned to balance energy consumption among nodes at intervals every corona. Liu et al. developed the integrated style of route

choice, traffic load allocation, and sleep planned to maximize the network lifetime. Supported the idea of expedient routing, developed a routing metric to deal with each link reliableness and node residual energy. The detector node computes the best metric price during a localized space to achieve each reliableness and lifetime optimization.

3. FRAMEWORK

The proposed CASER framework, the network is equally divided into little grids. Every grid incorporates a relative location supported the grid information. The node in every grid with the best energy state is chosen because the head node for message forwarding. additionally, every node within the grid can maintain its own attributes, as well as location information, remaining energy state of its grid, further because the attributes of its adjacent neighboring grids. The data maintained by every sensor node are updated intermittently.

A. System Overview

In this paper we implemented new scheme named as CASER. Here the data that is used for the secure transmission is energy balancing. Hence progress of the proposed scheme is used for the energy balancing and for secure transmission. A secure and efficient rate mindful at ease Routing (CASER) protocol is used to deal with energy steadiness and routing security at the same time in WSNs. In CASER routing protocol, every sensor node wishes to hold the energy stages of its immediate adjoining neighboring grids moreover to their relative locations. Utilizing this expertise, each sensor node can create various filters established on the expected design alternate-off between security and efficiency.

The quantitative security analysis described that the proposed algorithm can preserve the source place understanding from the adversaries. In this venture, we will focal point on two routing methods for message forwarding: shortest route message forwarding, and secure message forwarding by means of random walking to create routing course unpredictability for source privacy and jamming prevention.

B. System Architecture

Our proposed protocol works based on two adjustable parameters those are:

1. Energy Balance Control (EBC)
2. Random Walking

The EBC is the energy balance control; it's used to calculate the energy. The energy is calculating based on the EBC algorithm. First prefer the neighboring node for message forwarding. If the node is has the very best node approach select that node. The sink node has the knowledge about the whole node, that information is stored to the sink node. The source node sends the message to neighboring nodes, then transfer to the subsequent neighboring node. Eventually the message is send to sink node. In wireless sensor network, sink node has the all node knowledge. The EBC procedure is used to calculate the energy for the sensor node.

C. Deterministic Routing Strategy

i. Energy Balance Control (EBC):

According this paper, we have a major challenge i.e., network lifetime. By using EBC parameter, in the wireless sensor networks we can balance the energy levels of the sensor nodes in the deterministic

routing. Each sensor node in the network initially deployed with same energy. The energy levels of sensor nodes are reduced when the sensor node sends message to sink node. During transmission, each sensor node must know the neighbor node remaining energy levels. Hence, based on energy levels it finds the next node to routing in every grid. i.e.,

1. First the sender node computes the average remaining energy levels of the adjacent neighboring grids.
2. Determine the candidate grid for the next routing sensor node. Here, candidate grid means which sensor node having more remaining energy that node will be selected by the sender node and grid of the selected node is called candidate grid.
3. Forward the message to the grid in the average remaining energies that is closest to the sink node and its relative location.

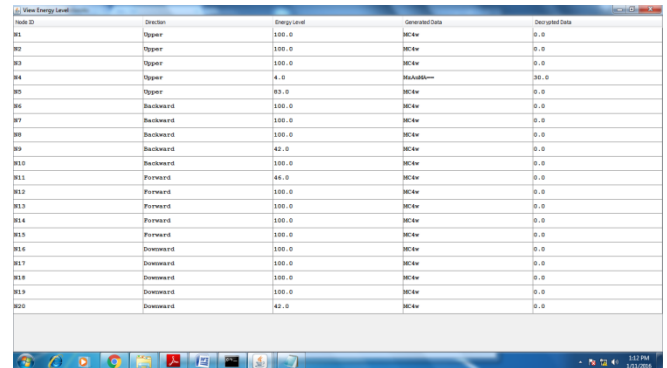
D. Random Walking Strategy

In random walking parameter, CASER protocol sends the messages with secure. When sender node sends the data to sink node, during transmission number of attacks are may occurred. So, in this protocol we implemented Random walking strategy.

In this strategy, once sender node sends the data to neighbor node then immediately the sender node will be blocked. By do like this we can protect the sender node details and also we can protect the data from the adversaries. In figure2 we can observe that the shaded area is hiding actual sender node and it displays another neighbor node as a sender in this strategy.

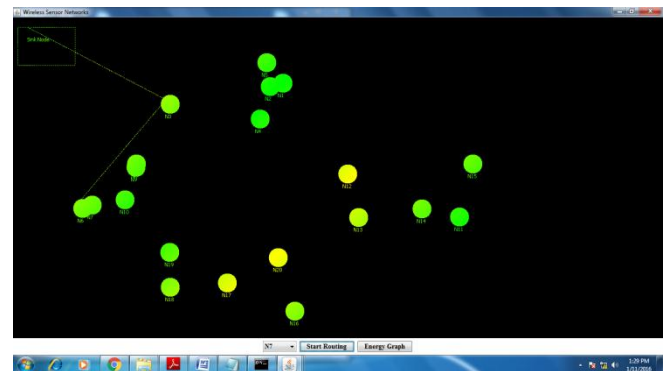
4. RESULT ANALYSIS

In the experiment, we need to check the initial energy levels of the sensor nodes. After, sending data from sender node it displays the remaining energy levels displayed. Below screen describes that the remaining energy levels of the sensor nodes in the network:



Node ID	Direction	EnergyLevel	Generated Data	Destroyed Data
N1	Upper	100.0	MC4e	0.0
N2	Upper	100.0	MC4e	0.0
N3	Upper	100.0	MC4e	0.0
N4	Upper	4.0	MC4e	100.0
N5	Upper	93.0	MC4e	0.0
N6	Backward	100.0	MC4e	0.0
N7	Backward	100.0	MC4e	0.0
N8	Backward	100.0	MC4e	0.0
N9	Backward	42.0	MC4e	0.0
N10	Backward	100.0	MC4e	0.0
N11	Forward	44.0	MC4e	0.0
N12	Forward	100.0	MC4e	0.0
N13	Forward	100.0	MC4e	0.0
N14	Forward	100.0	MC4e	0.0
N15	Forward	100.0	MC4e	0.0
N16	Downward	100.0	MC4e	0.0
N17	Downward	100.0	MC4e	0.0
N18	Downward	100.0	MC4e	0.0
N19	Downward	100.0	MC4e	0.0
N20	Downward	42.0	MC4e	0.0

In Deterministic routing, we can send the data from sender node to sink node with the balancing energy levels. Means it proved that our protocol significantly improves the network lifetime.



Through our experiments we can say our CASER protocol provides the high security as well as high message delivery ratio.

5. CONCLUSION

We conclude that in this paper, we present a secure and efficient CASER protocol for wireless sensor networks. By using this protocol we can balance the energy consumption and reduce network lifetime

optimization. CASER has the elasticity to support multiple routing schemes in message forwarding to enhance network lifetime while improving routing security.

REFERENCES

- [1] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012 2012.
- [2] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000.
- [3] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," UCLA Computer Science Department Technical Report, UCLACSD, May 2001.
- [4] C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F. Chou, and C.-J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, Aug. 2010, pp. 1–6.
- [5] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data gathering sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.
- [6] A. Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: issues and challenges," in The 8th International Conference on Advanced Communication Technology (ICACT), vol. 2, 2006, pp. 6 pp.–1048
- [7] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul. 2012.
- [8] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.
- [9] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, 2000, pp. 243–254.
- [10] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 120–130.