International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Improving Network Security and Enhancing the Network Lifetime for Achieving High Message Delivery Ratio

[1]Mrs.S.VISNU DHARSINI, [2] K. KUSUMA VENKATA RAMANI, [3]Y. SAI RATAN
[1]Faculty of Engineering, Department of CSE, SRM University, Ramapuram, Chennai
[2, 3] B. Tech Student, Department of CSE, SRM University, Ramapuram, Chennai

ABSTRACT— *while sending the data from sender to receiver we are suffering from lot of networking problems such as link breaks, packet drops, and energy consumption and so on. These major problems are mitigating network lifetime and security. Mainly, the network lifetime problem causes by the energy levels of the nodes in the network. In traditional systems, we used uniform energy deployment strategy. To that we cannot improve the network lifetime. In existing we have some protocol but they are not sufficient to resolve these two issues at a time. To overcome existing issues at a time in this paper, we propose Cost-Aware SEcure Routing (CASER) Protocol. Through this convention we can streamline the system lifetime alongside security. In this CASER convention we execute the uniform vitality organization methodology. This convention is extremely adaptable to expand the system lifetime and message sending.*

1. INTRODUCTION

A wireless Sensor Network (WSN) consists of loads or thousands of sensor nodes and a small range of information series devices. The sensor nodes have the form of low value, low-energy, small-length devices, and are designed to carry out a number sensing applications, including environmental monitoring, army surveillance, fire detection, animal monitoring, and so on. The sensor nodes collect the data of interest domestically and then ahead the sensed statistics over a wireless medium to a faraway facts collection tool (sink), in which it's miles fused and analyzed so that it will decide the worldwide status of the sensed region. In existing gadget geographic routing is used as the promising solution within the network. Geographic adaptive fidelity is used as the promising answer for the low energy sensor community .A question based geographic and electricity conscious routing was implemented for the dissemination of the node. In Geographic and Energy Aware Routing (GEAR), the sink disseminates requests with geographic attributes to the goal region rather than the use of flooding. Each node forwards messages to its neighboring nodes based at the envisioned price and the studying value. Source-place privateness is provided via broadcasting that combines legitimate messages now not handiest consumes good sized amount of sensor power. But additionally will increase the community collisions and decreases the packet transport ration. In phantom routing protocol each message is routed from the real supply to a phantom supply alongside a designed directed stroll via both quarter based technique or hop based totally method. The path area information is saved within the header of the message. In this manner, the phantom supply may be far away from the real supply. Unfortunately, once the message is captured at the random walk course, the adversaries

are able to get the path region data stored inside the header of the message.

Distributed Actor Recovery Algorithm (DARA) as well as PArtition Detection and Recovery Algorithm (PADRA) require every node to hold a report of their multi-hop associates and take a look at the scope of the restoration thru checking whether or not or not the failed nodes. Cost-Aware Secure Routing (CASER) protocol for WSNs to stability the electricity consumption and expand community lifetime. CASER has the elasticity to aid more than one routing techniques in message forwarding to extend the lifetime even as growing routing protection. Both theoretical analysis and simulation will exhibit that, CASER has a great routing performance in phrases of power balance and routing course distribution for routing route security. We additionally proposed a non-uniform strength deployment scheme to boom the sensor community lifetime. Our evaluation will showing that we are able to develop the lifetime and the number of messages that can be brought under the non-uniform power deployment by means of manner of extra than four activities. CASER supports comfortable transport, to preclude routing trackback attack and malicious web page visitors jamming attack in wireless Sensor conversation.

2. RELATED WORK

There is a growing interest inside the packages of WSANs inside the latest years. Due to the harsh hired environment and limited electricity deliver, WSAN is prone to be out of work, which may also break community connectivity. In this paper, Ke Yan, Guangchun Luo, Ling Tian, Qi Jia and Chengzong Peng look at the problem of restoring network connectivity when a unmarried node fails. A hybrid distributed, localized, and green connectivity recovery algorithm HCR is proposed to clear up this problem through shifting the backup node to BestPosition. Compared with the previous schemes, HCR performs a localized network analysis to become aware of crucial nodes, and handiest a important node's failure triggers the recuperation technique. It is a compromised inspiration among the cut vertex identity and non-identity. It is powerful and has low complexity. The performance of HCR is analyzed mathematically and established through simulations. The simulation consequences have showed the effectiveness of HCR in terms of all of the evaluation metrics. More importantly, HCR is applicable to diverse community topologies, sparse or dense. The performance of HCR stays strong when various network topology. Though a comprehensive network will growth the complexity of the choice of BestPosition, it's miles proper.

Prosenjit Bose, Pat Morin, Ivan Stojmenovi´c, and Jorge Urrutia have described algorithms for routing, broadcasting, and geocasting in unit graphs. The algorithms do now not require duplication of packets, or reminiscence at the nodes of the graph, and yet guarantee that a packet is constantly delivered to (all of) its destination(s). The empirical consequences for our routing algorithms suggest that although the face-1 and face-2 algorithms are not very efficient on their very own, they may be useful along with less complicated algorithms that don't guarantee shipping. There are numerous open issues and instructions for future paintings on this vicinity. One such direction is the extension of these designs to dynamically

changing networks. Although it's far viable to increase their algorithms with the desire of coping with dynamically changing networks, it isn't in any respect clear what's an affordable (mathematical or simulation) model under which to take a look at those modified algorithms.

Lata et al. Have supplied the at Secure Geographical Routing (SGR) algorithm for wireless sensor verbal exchange to decide occasion and sends knowledge to the lowest station. In preceding strategies, there was as soon as a disaster of transmitting more than one copies of the statistics packet via a couple of direction that consumes energy as opposed to a single reproduction of information transmission. They consider that the base station is located on the co-ordinates (0, zero) within the community area. The backside station has unlimited energy. Each and each node is categorized with a outstanding identity. Situated at the conversation distance, nodes have the capacity to adjust strength. They defined that the static and homogenous network version that works primarily based on "Collaborate, Collate & Compare" (CCC) formula. In that model cluster head offers and receives the statistics about its neighboring node. Within the SGR set of rules, first GPS nodes had been deployed alongside key with the well worth of x and y co-ordinates. Within the 2d step, information is probably accumulated. If the everyday well worth of the data is above than the threshold rate, then know-how transmission can be began. In third and very last step, worldwide and close by broadcast will possibly be used. Nearby broadcast guarantees supply of information from one node to the subsequent node securely; whereas, global set of rules ensures end-to-finish connectivity among sender and base station; to decorate the consistency, if an acknowledgment will now not be received, but a duplicate of expertise will probably be transmitted from an extra course.

Durrani et al. has provided the Trust-based Energy Efficient Secure Routing (TEESR) protocol. They highlighted the demanding situations, routing safety threats, specifications, and evaluation of current options. This protocol has a limited quantity of forwarding nodes, floods the buddies expertise in a small amount of messages as in assessment with other routing protocols. Consequently, the proposed scheme reduces end-to-end prolong and saves fantastic power.

3. FRAMEWORK

A. System Overview

In this paper, we plan a convention i.e., CASER convention. To apply this convention in the remote sensor arranges at first we have to plan the system. The system will be apportioned as lattices. In every framework comparable sensor hubs are sent. For all sensor hubs single goal that is sink hub. It implies the sink hub is goal for all sensor hubs. The information of the sink hub is made open. For security purposes, each message can be allotted a hub character relating to the area the place this message is started. To keep foes from enhancing the source area from the hub character, a dynamic id can be used. The content of each message can also be encrypted making use of the key shared between the node/grid and the sink node. We also anticipate that every sensor node is aware of its relative vicinity within the sensor area and has competencies of its instant adjoining neighboring grids and their vigor levels of the grid.

The understanding concerning the relative area of the sensor domain could also be broadcasted within the network for routing data replace.

B. CASER Protocol Routing Strategies

In this protocol, two kinds of strategies are there:

1. Deterministic Routing Strategy
2. Random Walk Routing Strategy

Actually, the CASER protocol works based on two adjustable routing parameters such as follows:

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

Deterministic Routing Strategy:

In deterministic routing, we use the EBC parameter. In this method we put into effect the non-uniform strength deployment strategy. In this method, first of all all sensor nodes have the identical strength and after a while they lose few amount of energy. Remaining energies are we want to calculate first. After that we should pick out the candidate grids.

Candidate grids manner based on calculated strength tiers of sensor nodes; in each grid we've one excessive strength degree node. We select that node to routing and that node's grid called a candidate grid. Based on selected candidate grids we formulate a shortest course. Through that shortest course we are sending the statistics. Finally, we are able to preserve the energy degrees of the sensor nodes within the network. Like this, we will optimize the community lifetime efficaciously inside the wireless sensor networks.

Random Walking Routing Strategy:

In random strolling parameter, CASER protocol sends the messages with comfy. When sender node sends the statistics to sink node, during transmission range of assaults are may additionally passed off. So, on this protocol we carried out Random strolling strategy. To provide the safety we pick the random stroll routing approach. It no longer only affords the safety to the node however also it controlled the power degrees.

In random stroll routing method, whilst we ship the facts via the shortest path it's going to now not shows the sender node to guard the node details and corresponding information from the hackers. It simply hides the real sender node info and it displays the nearest node of the sender node as a sender node. By enforcing likewise, there's no opportunity to the attacker to get the sender node information.

In this paper, first we manage the strength levels of the sensor nodes. When we are controlled the sensor nodes power stages in the community, then mechanically, we optimize the network lifetime. If network lifetime is elevated, then we will increase the excessive message shipping ratio in the wireless sensor networks. Through the Random walk approach we will attain the security issue additionally at a time within the routing.

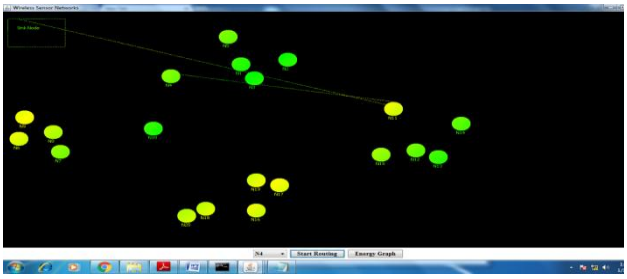
C. CASER Algorithm

Algorithm Node A finds the next hop routing grid based on the given parameters $\alpha, \beta \in [0, 1]$

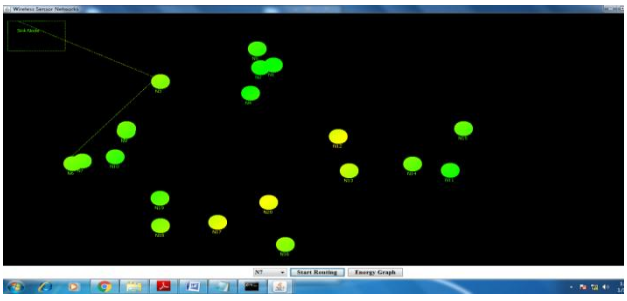
1: Compute the average remaining energy of the adjacent neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|} \sum_{i \in \mathcal{N}_A} \mathcal{E}r_i$.
2: Determine the candidate grids for the next routing hop: $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha \mathcal{E}_a(A)\}$.
3: Select a random number $\gamma \in [0, 1]$.
4: **if** $\gamma > \beta$ **then**
5: Send the message to the grid in the $\mathcal{N}_A^\alpha$ that is closest to the sink node based on its relative location.
6: **else**
7: Route the message to a randomly selected grid in the set $\mathcal{N}_A^\alpha$.
8: **end if**

4. EXPERIMENTAL RESULTS

In this experiment, we partition the network as grids. And after, we can check the initial energy levels of the sensor nodes. We can send data from sender node it displays the remaining energy levels of the routing nodes in every grid.

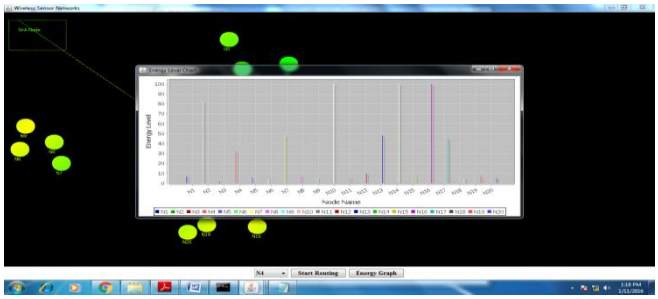


In Deterministic routing, we can send the data from sender node to sink node with the balancing energy levels. Means it proved that our protocol significantly improves the network lifetime.



After, send the data we can check the remaining energy levels of the routing nodes in the network as a energy graph.

In secure random walk strategy, the sender node will be hided.



From the 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 address two network challenges such as network security and network lifetime optimization. These two challenges are addressed by the CASER protocol which is provided security along with node energy balancing in the wireless sensor network. From the experimental results we proved that the proposed CASER protocol achieved high message delivery ratio and energy balancing.

6. FUTURE ENHANCEMENT

CASER lets in messages to be transmitted using two routing strategies, random walking and deterministic routing, within the same framework. In the Random taking walks approach, there's a hazard of choosing low strength node as a relay node. To keep away from this, the facts is transmitted via power aware

direction handiest, the MES scheme on Elliptic curve algorithm used to provide authentication. For safety functions, the content of every message also can be encoded with the aid of the use of sample encoding technique and decoded on the sink node by means of knowing the swapping bit function. So, unauthenticated character cannot get admission to the authentic data. By this manner, the protocol gives a relaxed message transport choice to maximize the message shipping ratio underneath adverse attacks.

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.