DESIGNING COST – EFFICIENT SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

T. Panchajanyam[1], Dr. M Nagaratna[2]
[1]M. Tech Student, [2]Assistant Professor
Department of CSE, Jawaharlal Nehru Technological University Hyderabad College of Engineering, Village KPHB, Mandal Kukatpally, District RangaReddy, Telangana, India.

Abstract: A wireless sensor network (WSN) can be defined as a spatially distributed and autonomous sensors to envision the physical or the environmental conditions, like temperature, sound, pressure, Humidity etc. Routing is a challenging design issue for Wireless Sensor Networks because of Network Lifetime Optimization and Security for the multi-hoping in WSN's. A Perfectly designed routing protocol should not only ensure for high message delivery ratio and low energy consumption for a message delivery, but it should also balance the entire sensor network power consumption, and it should extend the lifetime of sensor network. This paper is proposed a secure and efficient Cost-Aware and Secure Routing (CASER) protocol to resolve these two conflicting issues by two adjustable parameters. Those are: Energy Balance Control (EBC) and Probabilistic-Based Random Walking. It will discover that the energy consumption is severely disproportional to uniform energy deployment for a given network topology, which almost reduces the lifetime of the sensor networks. To resolve this problem, we propose an efficient and non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under a same energy resource and security requirement. For the non-uniform energy deployment, our analysis shows that this can increase the network lifetime and the total number of messages that can be delivered by more than four times under the same assumption.

Index Terms: Message Delivery, CASER, Energy balance control, Random walking, Energy deployment, Energy consumption;

I. INTRODUCTION

The recent technological advances build wireless sensor networks (WSNs) technically and economically possible to be wide employed in each military and civilian application, like observance of close conditions associated with the setting, precious species and significant infrastructures. A key feature of such networks is that every network consists of an outsized range of unbound and unattended sensor nodes. These nodes typically have terribly restricted and non-replenish able energy resources, which makes energy a very important design issue for these networks. Routing is another terribly challenging design issue for the WSNs. A properly designed routing protocol mustn't solely guarantee a high message delivery ratio and low energy consumption for message delivery, however conjointly balance the whole sensor network energy consumption, and thereby extend the sensor network life. CASER protocol has two major advantages: (i) it ensures balanced energy consumption of the entire sensor network in order that the life of the WSNs may be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing needs, including fast/slow message delivery and secure message delivery to forestall routing trace back attacks and malicious traffic electronic countermeasures attacks in WSNs.

Characteristics of CASER Protocol:

- To maximize the sensor network time period, we ensure that the energy consumption of all sensor grids are balanced.
- To realize a high message delivery ratio, our routing protocol should attempt to avoid message dropping when an alternate routing path exists.
- The adversaries shouldn't be ready to get the source location data by analyzing the pattern.
- The adversaries shouldn't be ready to get the source location data if he is solely ready to monitor a certain space of the WSN and compromise many sensor nodes.
- Solely the sink node is ready to spot the source location through the message received. The recovery of the source location from the received message should be terribly efficient.
- The routing protocol ought to maximize the probability that the message is being delivered to the sink node once adversaries are solely ready to jam a few sensing element nodes.

An Efficient and a non-uniform energy deployment system to optimize lifetime and message delivery ratio under a same energy resource and a security requirement it can also provide a quantitative security analysis on the proposed routing protocol. It can provide a good trade-off between the routing efficiency and the energy balance, and can significantly enhance the lifetime of the sensor networks in all directions. For a non-uniform energy deployment, to maximize the lifetime and the maximum number of messages that can be delivered by more than four times by the same assumption. To get a high message delivery ratio while preventing the routing trace back attacks.

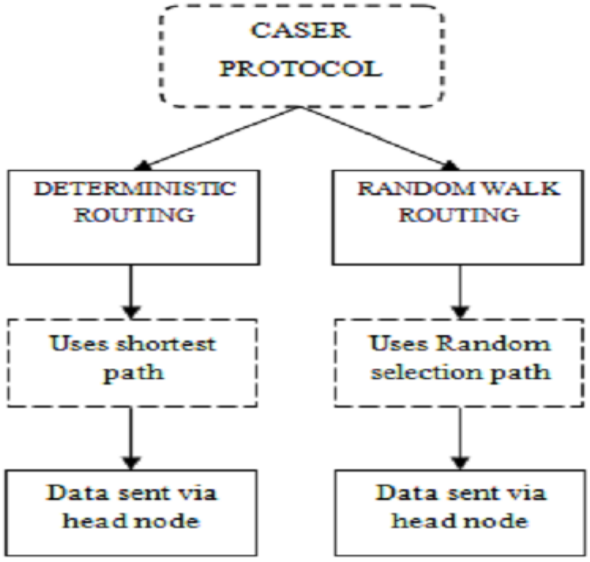


Figure.1. Levels of CASER Protocol

II. RELATED WORK

A wireless Sensor network includes a massive quantity of untethered and unattended sensor nodes. These nodes often have very restricted and non-replenish able energy resources, which makes an energy a most important design drawback for these networks. Routing is a different very difficult design limitation for WSNs. A properly designed routing protocol must now not be most effective make certain excessive message supply ratio and low energy consumption for message supply, but additionally steadiness the complete sensor network power consumption, and thereby lengthen the sensor community lifetime. In addition, the aforementioned issues, WSNs depend on wireless communications, which is by using nature a broadcast medium. It is more at risk of protection assaults than its wired counterpart because of lack of a physical boundary. In exact, in the wireless sensor domain, any person with an appropriate wireless receiver can monitor and intercept the sensor network communications. The adversaries may just use costly radio transceivers, powerful workstations and engage with the community from a distance since they are not restrained to making use of sensor community hardware. It's feasible for the adversaries to perform jamming and routing hint back assaults. While geographic routing algorithms have the benefits that each node simplest wants to preserve its neighboring information, and provide a bigger effectively and a greater scalability for massive scale WSNs, these algorithms could attain their neighborhood minimal, which is able to effect in useless finish or loops. Our broad OPNET simulation results exhibit that CASER can furnish best power balance and routing safety. It is also proven that the proposed comfortable routing can expand the message delivery ratio because of diminished dead ends and loops in message ahead.

The main drawbacks of existing system are:

- It cannot ensure balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.
- The secure message delivery does not to prevent routing trace back attacks and malicious traffic jamming attacks in WSNs.
- The energy consumption is severely disproportional to the uniform energy deployment for a given networking topology, which greatly reduces the lifetime of the sensor networks.

In this paper, for the first time, we tend to propose a secure and efficient Cost Aware SEcure Routing (CASER) protocol that can address the energy balance and the routing security at the same time in WSNs. In CASER protocol, every sensing element node desires to manage the energy levels of its immediate adjacent neighboring grids additionally to their relative locations. Using this data, every sensing element node will produce variable filters support the expected design trade-off between security and potency. The quantitative security analysis demonstrates the proposed algorithmic rule will defend the source location data from the adversaries. Our in depth OPNET simulation results show that CASER will offer excellent energy balance and routing security. It's additionally incontestable that the proposed secure routing will increase the message delivery quantitative relation attributable to reduced dead ends and loops in message forward.

III. FRAME WORK

A. The System Model

We count on that the WSNs are composed of a huge number of sensor nodes and a sink node. The sensor nodes are randomly deployed during the sensor area. Each sensor node has a very limited and non-replenishable power resource. The sink node is the best vacation spot for all sensor nodes to send messages to through a multi-hop routing approach. The information of the sink node is made public. For security functions, each message may also be assigned a node id corresponding to the region where this message is initiated. To save you adversaries from convalescing the source place from the node identity, a dynamic identification can be used. The content of every message can also be encrypted using the mystery key shared among the node/grid and the sink node. We additionally count on that each sensor node knows its relative place within the sensor domain and has knowledge of its instantaneous adjoining neighbouring grids and their electricity tiers of the grid. The data approximately the relative location of the sensor domain can be broadcasted within the network for routing facts replace. On this paper, we cannot deal with key management, consisting of key technology, key distribution and key updating.

B. Proposed System Overview

In our scheme, the network is evenly divided into small grids. Each grid has a relative region based totally on the grid statistics. The node in every grid with the very best strength level is chosen as the head node for the message warding. Similarly, each node within the grid will maintain its very own attributes which includes location statistics, remaining electricity degree of its grid, as well as attributes of its adjoining neighbouring grids. The information maintained by way of each sensor node could be up to date periodically. We expect that sensor nodes in its direct neighbouring grids

are all within its direct conversation range. We additionally count on that the complete network is absolutely linked through multi-hop communications. While maximizing message source location privateness and minimizing visitors jamming for communications between the supply and the vacation spot nodes, we can optimize the sensor community lifetime through a balanced energy intake all through the sensor community. Further, the maintained strength stages of its adjacent neighbouring grids may be used to come across and clear out the compromised nodes for lively routing choice.

C. Energy Balance Control

To balance the overall sensor device power consumption in all grids with the aid of controlling electricity going thru from sensor hubs with low electricity ranges. The source hub sends the message to neighbouring hubs, then move to the following neighbouring hub. The Figure 2 demonstrates that, the data is acquired by using the vacation spot node from the source node in view of the neighbor's node choice. The EBC is the energy balance control; this is utilized to figure the strength. The power is ascertaining considering the EBC set of rules. First of all choose the neighboring hub for message forwarding. On the off chance that the node/hub has the most expanded hub implies pick out that hub. The sink hub has the facts about the entire hub, that statistics is put away to the sink hub. The source hub sends the message to neighbouring hubs, then move to the subsequent neighbouring hub. At long ultimate the message is send to sink hub. In far flung sensor network, sink hub has the all hub facts. The EBC method is applied to determine the power for the sensor hub.

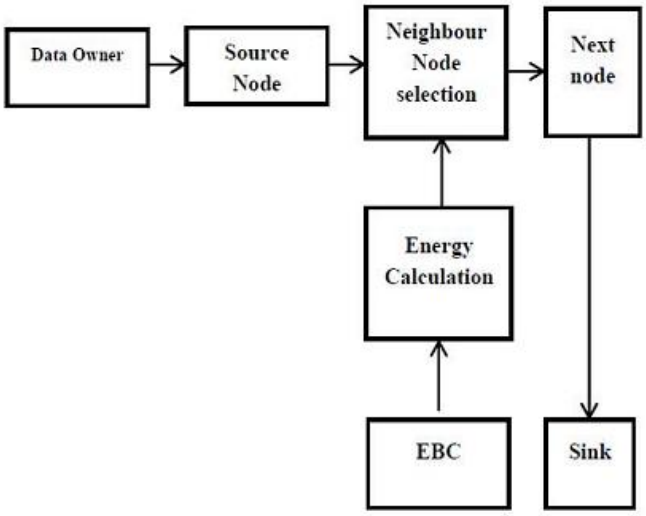


Figure.2. System Overview

D. Routing with Balanced Energy

In the choice of the neighbouring node selection the power degree of each node to be taken into consideration to reap the strength stability, display and manipulate the electricity intake for the nodes with exceptionally low power tiers. To choose the grids with relatively better final strength tiers for message forwarding. It may be effortlessly seen that a larger A corresponds to a better EBC. It is also clear that growing of a main additionally they increase the routing period it can effectively manage energy consumption from the nodes with strength ranges decrease than A. The CASER direction selection calculation is derived by means of the equation

$$\varepsilon_a(A)=\frac{1}{\|N_A\|}\sum_{i\epsilon N_A}\varepsilon_{r_i}.$$

Here ε is a parameter used for Energy Balance Control. And after that the term α is used to signify testing proportion. On the off chance that α quality is most extreme means there is no shortest path in that hub.

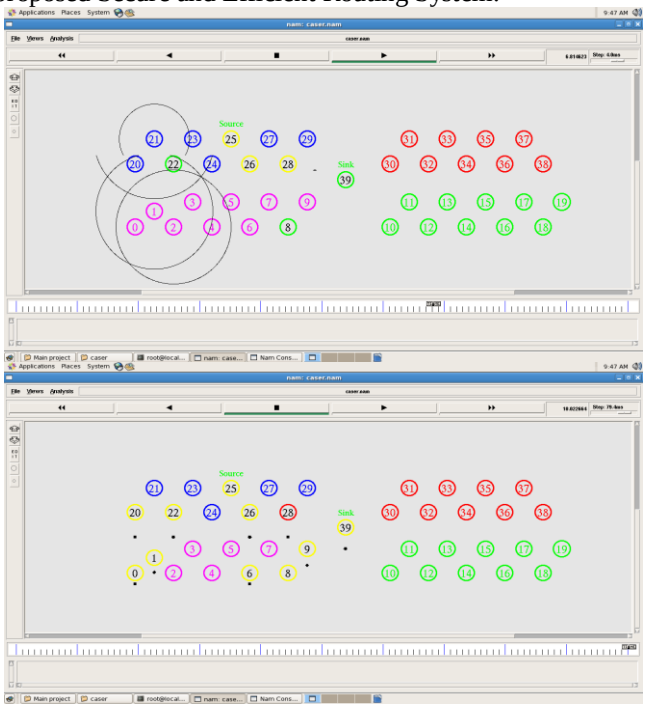
E. A Secure Routing using CASER Protocol

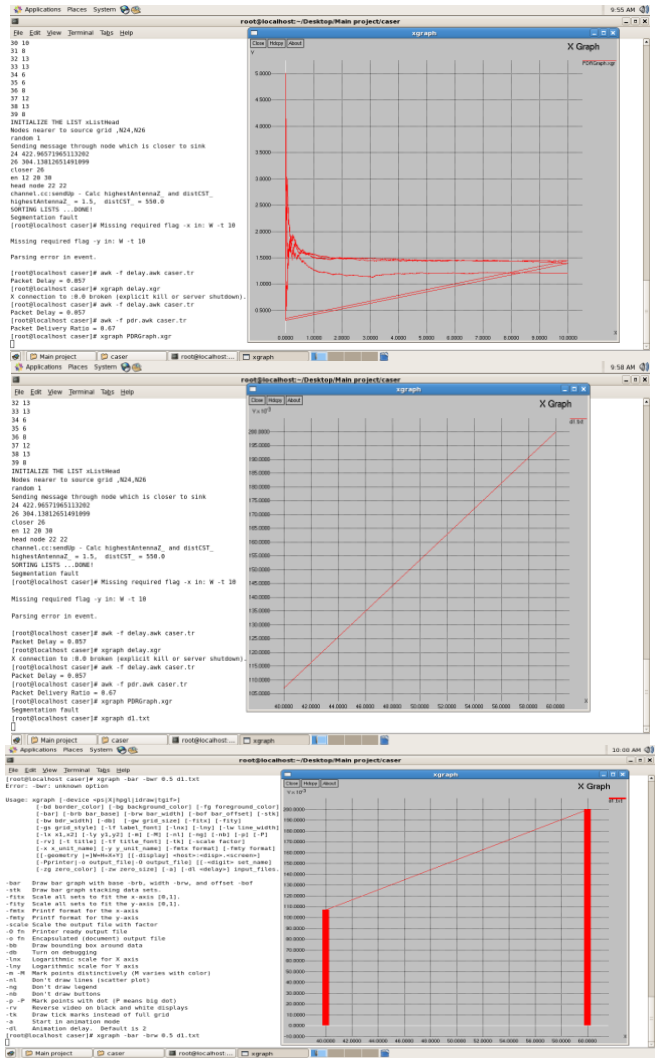
Within the proposed model the data which can be transmitted according to the routing strategy. A Routing Strategy that can offer routing path unpredictability and a safety. The routing direction emerge as greater changeable. A Routing Protocol consists of two alternatives for message forwarding: one is a deterministic shortest direction routing grid selection algorithm, and the other is a at ease routing grid selection set of rules via random walking. In the deterministic routing technique, the subsequent hop grid is selected from N_A^{α} primarily based on the relative places of the grids. The grid that is closest to the sink node is chosen for message forwarding. Inside the secure routing case, the subsequent hop grid is randomly selected from N_A^{α} or message forwarding. The distribution of those two algorithms is managed by means of a security stage called β∈[0,1], carried in every message.

IV. EXPERIMENTAL RESULTS

We have implemented our model in Network Simulator 2. We have conducted an experiment to analyze the routing performance a proposed CASER Protocol for four different issues such as routing path, energy balancing, and total number of messages that can be delivered and a delivery ratio of messages under same energy consuming ratio.

The Screens given below show the experimental result of the proposed Secure and Efficient Routing System.





V. CONCLUSION

From this paper, we present a secure and efficient Cost Aware SEcure Routing (CASER) protocol for Wireless Sensor Networks to reduce the energy consumption and increase lifetime of networks. CASER is flexible to support several routing strategies in message forwarding to increase lifetime and, while increasing the routing security. Both the theoretical analysis and simulation results prove that CASER has very good routing performance if we consider the energy balancing and a routing path distribution for a path security. We have also proposed a non-uniform energy deployment approach to maximize the sensor network lifetime. Analysis and Simulation results show that we can extend the lifetime and the number of messages to be delivered by the non-uniform energy deployment.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks," Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," Comput. Sci. Dept., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00-729, Apr. 2000.

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., 1999, pp. 48–55.

[10] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd ACM Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., Seattle, WA, USA, Aug. 1999, pp. 48–55.

[11] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2004, vol. 3, pp. 1705–1716.

[12] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[13] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 17–21, 2002, vol. 1, pp. 350–355.

