International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 12
ISSN: 2454-4248
339 – 343

Energy Balance Control and Security for Wireless Sensor Network by Using Cost-Aware Secure Routing protocol

Rashmi D. Gaikwad[1]
M. Tech Scholar
B.I.T. Ballarpur, Chandrapur
rashmigaikwad1307@gmail.com

Prof. Sagar Bhakre[2]
Assistant Professor
B.I.T. Ballarpur, Chandrapur
bhakresagar@gmail.com

Abstract: Reliability, Energy balance and security are conflicting design issues for wireless sensor networks (WSNs) with non-replenishable energy resources. In this paper, we first propose a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic- based random walking.

To solve this problem, we propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. We also provide a quantitative security analysis on the proposed routing protocol. For the non-uniform energy deployment, our analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. We also demonstrate that the proposed CASER protocol can achieve a high message delivery ratio while preventing routing traceback attacks.

Keywords:*-(EBC) energy balance,,Cost-Aware SEcure Routing (CASER)*

*****

I. INTRODUCTION

A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.[1] The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.[1]

In addition to one or more sensors, each node in a sensor network is typically equipped with a radiotransceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The size a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust.[1] The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes.[1] Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.[1]

Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. Motivated by the fact that WSNs routing is often geography-based secure and efficient Cost-Aware secure routing (CASER) protocol for WSNs without relying on flooding CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements.

II. EXISTING SYSTEM

In existing system geographic routing is used as the promising solution in the network. Geographic adaptive fidelity is used as the promising solution for the low power sensor network .A query based geographic and energy aware 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 target region instead of using flooding. Each node forwards messages to its neighboring nodes based on the estimated cost and the learning cost. Source-location privacy is provided through broadcasting that mixes valid messages not only consumes significant amount of sensor energy. But also increases the network collisions and decreases the packet delivery ration. In phantom routing protocol each message is routed from the actual source to a phantom source along a designed directed walk through either sector based approach or hop based approach. The direction sector information is stored in the header of the message. In this

 ISSN: 2454-4248
339 – 343

way, the phantom source can be away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries are able to get the direction.

III. PROPOSED SYSTEM

To overcome this drawback new scheme is implemented and named as CASER. Here the data that is used for the secure transmission is energy balancing. Thus development of the proposed scheme is used for the energy balancing and for secure transmission. A secure and efficient Cost Aware Secure Routing (CASER) protocol is used to address energy balance and routing security concurrently in WSNs. In CASER routing protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design trade-off between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. In this project, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention.

Energy Balance Control (EBC)

To balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels.

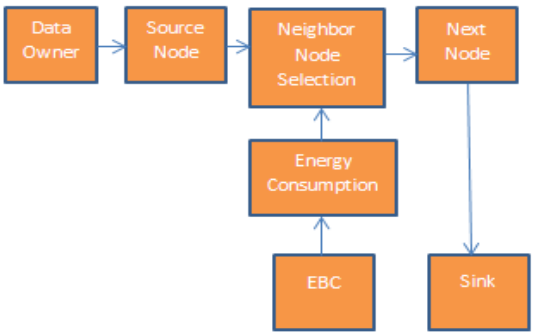


Figure :- Energy Balance Control System

The source node sends the message to neighboring nodes, then move to the next neighboring node.

System Overview

The above figure shows that, the data is sent the source node to destination node based on the neighbor's node selection. The EBC is the Energy Balance control; it is used to calculate the energy. The energy is calculating based on the EBC algorithm. First select the neighboring node for message forwarding. If the node is has the highest node means select that node. The sink node has the information about the entire node, that information is stored to the sink node. The source node sends the message to neighboring nodes, then move to the next neighboring node. Finally the message is send to sink node. In wireless sensor network, sink node has the all node information. The EBC method is used to calculate the energy for the sensor node.

CASER Routing

We propose a secure and efficient Cost Aware Secure Routing (CASER) protocol that can address energy balance and routing security concurrently in WSNs. In CASER routing protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design tradeoff between security and efficiency. we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention

We now describe the proposed CASER protocol. Under the CASER protocol, routing decisions can vary to emphasize different routing strategies. In this paper, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention. As described before, we are interested in routing schemes thatcan balance energy consumption.

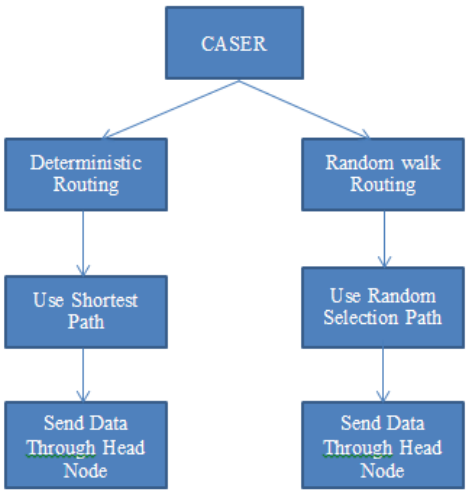


Figure: CASER Protocol Routing

Assumptions and Energy Balance Routing

In the CASER protocol, we assume that each node maintains its relative location and the remaining energy levels of its immediate adjacent neighboring grids. For node A, denote the set of its immediate adjacent neighboring grids as $N_A$and the remaining energy of grid i as €ri, i € N_A.

 ISSN: 2454-4248
339 – 343

With this information, the node A can compute the average remaining energy of the grids in N_A as $\epsilon a(A)=\frac{1}{NA}\sum_{i\epsilon NA}\epsilon ri$

In the multi-hop routing protocol, node A selects its next hop grid only from the set N_A according to the predetermined routing strategy. To achieve energy balance among all the grids in the sensor network, we carefully monitor and control the energy consumption for the nodes with relatively low energy levels by configuring A to only select the grids with relatively higher remaining energy levels for message forwarding.

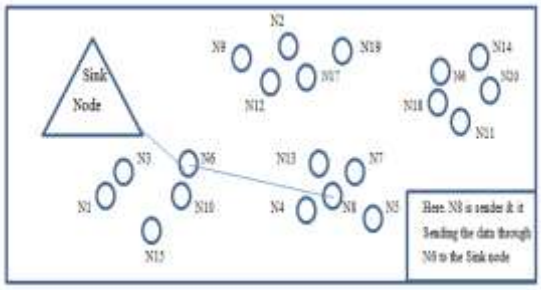
The System Model

We assume that the WSNs are composed of a large number of sensor nodes and a sink node. The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node has a very limited and non-replenishable energy resource. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy. The information of the sink node is made public. For security purposes, each message may also be assigned a node ID corresponding to the location where this message is initiated. To prevent adversaries from recovering the source location from the node ID, a dynamic ID can be used. The content of each message can also be encrypted using the secret key shared between the node/grid and the sink node. We also assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels of the grid. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update. In this paper, we will not deal with key management, including key generation, key distribution and key updating.

System Work

In our theme, the network is equally divided into little grids. Each grid incorporates a relative location supported the grid data. The node in each grid with the best energy level is chosen as a result of the head node for message forwarding. To enhance, each node inside the grid will maintain its own attributes, as well as location data, remaining energy level of its grid, additional as a result of the attributes of its adjacent neighboring grids. The data maintained by each sensor node are updated intermittently.

System Design: during this paper, we tend to design a protocol i.e., CASER protocol. To use this protocol within the wireless sensor network at first we need to design the network. In figure1, we tend to consider that in our network we have additional range of sensors and one sink node. During this network are going to be partitioned as grids. In every grid equivalent sensor nodes are deployed. From the figure, we have four grids and in each grid have five sensor nodes. For complete network we have only single sink node.



It suggests that the sink node is simply destination for all sensor nodes. The data of the sink node is made public. For security functions, each message will be assigned a node identity equivalent to the situation the place this message is initiated. To prevent adversaries from raising the source location from the node identity, a dynamic id will be used. The content of every message also can be encrypted creating use of the key shared between the node/grid and therefore the sink node. We tend to additionally anticipate that each sensor node is attentive to its relative neighborhood among the sensor area and has competencies of its instant contiguous neighboring grids and their vigor levels of the grid. The understanding concerning the relative space of the sensor domain may even be broadcasted inside the network for routing data replace. Routing methods in CASER in this protocol, two types of methods are there: 1) Deterministic Routing Strategy and 2) Random Walk Routing Strategy.

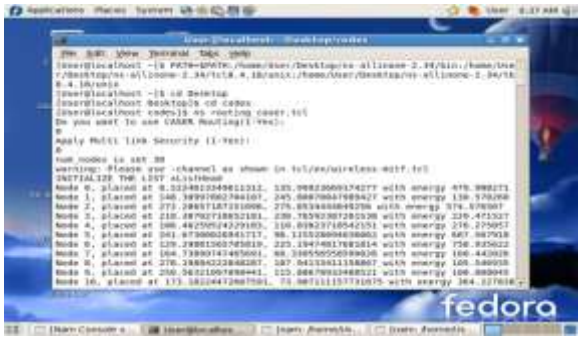
Design Goals

Our design goal can be summarized as follows:

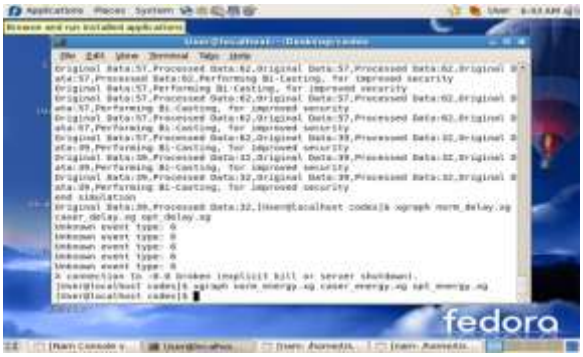
1. To maximize the sensor network lifetime, we ensure that the energy consumption of all sensor grids are balanced.
2. To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.
3. The adversaries should not be able to get the source location information by analyzing the traffic pattern.
4. The adversaries should not be able to get the source location information if he is only able to monitor a certain area of the WSN and compromise a few sensor nodes.
5. Only the sink node is able to identify the source location through the message received. The recovery of the source location from the received message should be very efficient.
6. The routing protocol should maximize the probability that the message is being delivered to the sink node when adversaries are only able to jam a few sensor nodes.

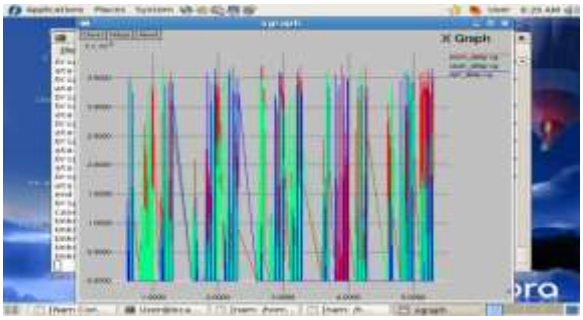
ISSN: 2454-4248
339 – 343

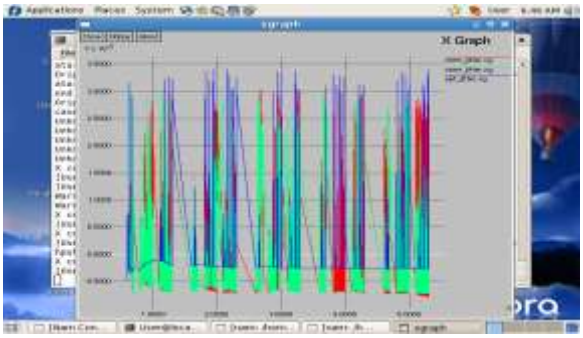
Result of Proposed Method

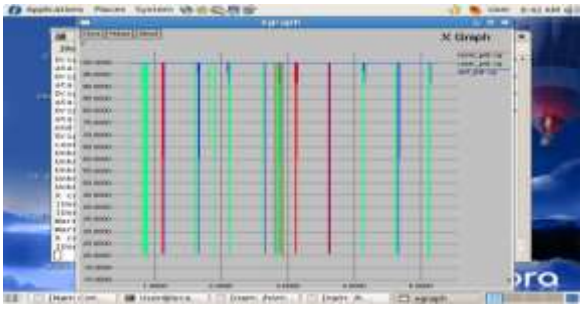


Execution of CASER Protocol for Graph









 ISSN: 2454-4248
339 – 343

Scope of Future work

The Simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. This also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. Our analysis and simulation results show that we can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four times.

Application of the proposed work will be

- Environmental monitoring
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

IV. CONCLUSION

We conclude that in this project, we tend to present a secure and efficient Cost-Aware Secure Routing (CASER) protocol for wireless sensor networks. By using this protocol we will balance the energy consumption and reduce network lifetime improvement. Cost-Aware Secure Routing protocol has the flexibility to support multiple routing schemes in message forwarding to support network lifetime whereas improving routing security.

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.

[14] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 609–619, Aug. 2004.

[15] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," IEEE Trans. Parallel Distrib.Syst., vol. 20, no. 10, pp. 1526–1539, Oct.2009.