International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 6 –OCTOBER 2016 (SPECIAL ISSUE)

Energy Optimized Secure Routing (EOSER) Protocol for Wireless Sensor Network

Syed Amer Mohiuddin and Prof. Shridevi Soma

PG scholar, Computer Network Engineering, PDA College of Engineering, Kalaburagi, India

Assoc. Professor, Computer Science and Engineering, PDA College of Engineering, Kalaburagi, India

***Abstract*— The major advancement in technologies results in security and energy efficiency issues in large wireless sensor networks. To solve those issues a protocol known as Energy Optimized Secure Routing (EOSER) is designed which uses two adjustable parameters: (EBC) Energy Balanced Consumption and (PRW) Probabilistic Random Walk routing. The energy consumption of devices are directly proportional to the uniform energy deployment of given topology, this problem is solved in this work using scattered energy deployment strategy to increase message delivery ratio and lifetime of the topology. From our experiment and simulation results the proposed (EOSER) protocol can provide a great tradeoff between routing efficiency and energy consumption. The proposed protocol can also be used to increase message delivery ratio by preventing trace back attacks.**

Index Terms— Energy Optimization, Security, Delivery Ratio, Non-uniform Energy Deployment, Source Location Privacy

I. INTRODUCTION

The recent technical advances make wireless sensor networks (WSNs) technically and inexpensively feasible to be widely used in both armed and civilian applications, such as keeping eye on ambient conditions related to the environment, precious species and critical designs. These nodes often have very limited and non-recoverable energy resources, which makes energy an important design issue for these networks. Routing is another very tricky design issue for WSNs for that a correctly 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 utilization, and thereby extend the sensor network lifetime. In addition to the abovementioned issues, WSNs rely on wireless communications, which is by nature a broadcast medium. It is more susceptible to security attacks than its wired equivalent due to lack of a physical limit. In particular, in the wireless sensor domain, anybody with an suitable wireless receiver can monitor and interrupt the sensor network communications. The hackers may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not constrained to using sensor network hardware. It is possible for the hackers to perform jamming and routing trace back attacks. Aggravated by the fact that WSNs routing is often topography- based, we propose a topography-based secure and efficient Energy Optimized Secure Routing (EOSER) protocol for WSNs without depending on flooding. EOSER allows messages to be transmitting using two routing strategies, random walking and deterministic routing, in the same framework. The sharing of these two strategies is determined by the specific security necessities. The protocol also provides a secure message delivery option to make the most of the message delivery ratio under adversarial attacks.

The paper is organized as follows. In section II related works are discussed. Section III describes modules of the proposed work. Section IV shows the simple architecture of the system. In Section V, performance and the results of proposed scheme are discussed and finally section VI concludes the proposed system.

II. RELATED WORK

Routing the message is a tricky task in WSNs due to the narrow resources. Geographic routing has been broadly viewed as one of the most gifted approaches for wireless sensor network [1]. In the Geographic routing protocols information is routed hop-by-hop from the source to the destination. The source node chooses the immediate neighboring node to forward the message based on either the routing path or the distance. The distance between the neighboring nodes can be calculated by signal strengths or using GPS equipments. The relative location information can be exchanged between neighboring nodes.

A. Geographical Routing Based

In [5], a geographic adaptive fidelity (GAF) routing scheme was proposed for sensor networks equipped with low power GPS receivers. In GAF, the network area is divided into predetermined size virtual grids. In each grid, only one node is selected as the active node, while the remaining will sleep for a period to save energy. The sensor for-wards the messages based on greedy geographic routing strategy. A query based geographic and energy aware routing (GEAR) was proposed in [6]. In GEAR, the sink node sends requests with geographic information to the target region instead of using flooding. Each node pass

the messages to its neighboring nodes based on expected cost and learning cost. The expected cost considers both the distance to the destination and the remaining energy of the sensor nodes. The learning cost provides the updated information to handle local minimum problem.

B. Privacy Based Source Location

In this scenario the source location privacy is provided by broadcasting that mixture of valid messages with dummy messages. The main proposal is that each node needs to transmit messages consistently. If there is no valid message to transmit, the node should transmit dummy messages. The broadcast of dummy messages not only consumes significant amount of sensor energy, but also overload the network and increases the packet collisions and decreases the packet delivery ratio. In phantom routing protocol [22], each message is routed from the authentic source to a dummy source along a premeditated walk through either sector-based approach or hop-based approach. The routing information is stored in the header of the message. Then every forwarder on the random walk path forwards this message to a random neighbor based on the route determined by the source node.

III. SYSTEM MODEL

The proposed scheme has the following system assumptions those are following in proposed scheme are given below:

A. System Model Assumption

Several assumptions has to be made before going to proposed the system that is we consider the wireless sensor network consist of large no nodes with limited energy resources, Hence nodes are wireless they can arbitrarily placed in the domain.

Here we have only one sink node the information of the sink node is made public and the sink node is the only destination for all the source nodes. Each node is assigned by node ID for security issues to know the initialization of the message. Each message may be encrypted to secure the data malfunction from the hackers. We also assume each node knows its relative location in the grid and it is updated by its intermediate nodes time to time.

The source location privacy is major concern with reference to the security issues, the hackers try to retrieve the source of message by jamming the sink node while we assume hackers might have major advantage over sensor devices, they may have highly equipped devices huge energy sources, high computational capability and high storage devices. Hackers may directly know the location of the sender by tracking the signal strength and direction of the message and can reach the destination with less delay. Even hackers can monitor the traffic of entire WSN.

B. Designed Goals

The goals to be achieved by proposed system are as follows:

1) Increasing the lifetime of the wireless Sensor network by using non uniform energy deployment scheme.
2) Source location privacy is achieved by using secure random walk routing strategy.
3) Increase the message delivery ratio by avoiding the collision by eliminating dummy messages and reducing the traffic on the network.

C. Proposed System

A novel and secure energy optimized secure routing (EOSER) protocol is proposed which optimizes the energy of the nodes and enhances the security of the network. The entire network is divided into different regions and each region is known as a grid, each grid consist of n no of nodes out of which one node is selected as active node or the head node , all remaining nodes are in the sleep mode to save the energy of the grid. A non-uniform energy deployment scheme is used to save the energy of the network and along with that security is also a major concern for that a source location privacy scheme is used. The source location of sender node is hided from the advisors by sending messages through random walk routing. Deterministic routing is used to send packets through shortest path which is predefined.

IV. ARCHITECTURE

The simple architecture of the proposed protocol is shown below:

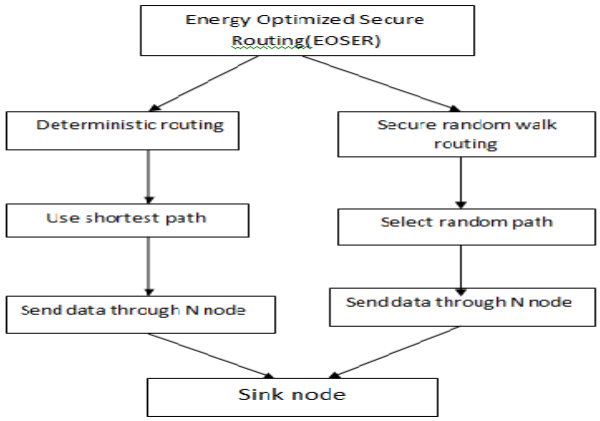

Fig-1: Architecture of Energy Optimized Secure Routing (EOSER) protocol.

The Energy Optimized Secure Routing protocol uses two routing strategies to forward the message to the destination based on the type of routing is selected it perform the operations. If the random walk routing is selected the proposed protocol hide the source from hackers to get the information of the source and send the data to the destination through a randomly selected node through the active head node. If deterministic routing is selected then it uses shortest path first routing strategy to send the data to the destination.

Energy Optimized Secure Routing (EOSER) protocol

This section provides the details of EOSER.

A. Algorithms used

We majorly perform computation of energy of the grid and next hop routing grid based on the energy balance parameter E which is illustrated in the algorithm

Algorithm 1: Node A finds the next hop routing grid based on the EBC.
Input: All nodes in the nodes in the wireless sensor network.
Output: Node with highest energy level.
Start
Step1. Compute the average remaining energy of the adjacent neighboring grids
Determine the candidate grids for the next routing hop.

$$\frac{1}{na}\sum_{i\in NA} \square\square i . \frac{1}{na}\sum_{i\in NA} \square\square i .$$

Step2. Determine the candidate grids for the next routing hop.

step3. Send the message to the node in the grid closest to the sink node based on its relative location.
Stop

Algorithm 2: Finding the next hop routing grid based on the giver parameters.
Input: All nodes in the nodes in the wireless sensor network.
Output: node with highest energy level and close to sink node.
Start
Step1. Compute the average remaining energy of the adjacent neighboring grids .
Step2. Determine the candidate grids for the next routing hop.
Step3. Select the random number ɤ€ (0, 1).
Step4. Send the message to the grid closest to the sink node.
Step6. Route the message to a randomly selected grid in the set A.
Stop

In Algorithm1 we try to compute energy of each grid in a wireless sensor networks. And elect one node as the head node based on closest to the receiver and the node should have highest energy level. The remaining nodes in a grid will became inactive till they receive the message from the active node. Hence they save energy to optimize the lifetime of the network. Here E denotes the energy of the grid. Na denotes neighboring node.

The second algorithm finds the next hop node to the destination by calculating the energy left in a node and closest node to the receiver. Er denotes the remaining energy in the grid. The algorithm tries to determine the relative location of the grid which is closest to the dink node by randomly selecting a grid the set A.

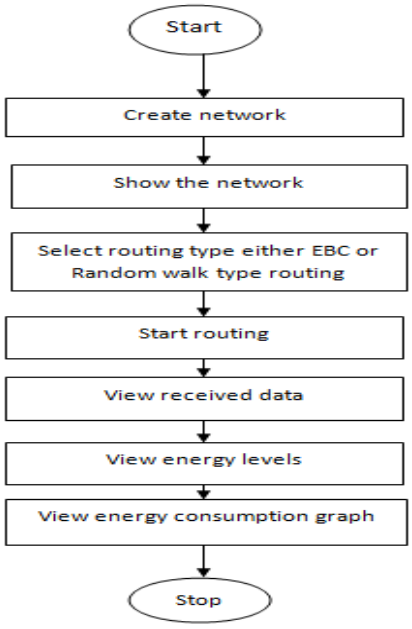

Fig- 2: Flow Diadram of EOSER algorithm.

The above figure shows the step by step execution of the simulation model designed for the proposed system. The above mentioned flow diagram shows the energy levels of the node and the energy consuption of each node used for the simulation. It also depicts the enire process and execution of the simulation used to show the practical implimentation of the proposed schemes and techniques.

B. Non-Uniform Energy Deployment

This scheme leads to minimize the energy consumption of the nodes and increase the lifetime of the wireless sensor network. As described by previous discussions the grid close to the sink node has high energy consumption then the nodes away from sink node. This non-uniform energy deployment scheme is used to conserve the energy of the nodes which are closer to the sink node. Redefine the energy consumption scenario and energy remaining calculation to avoid the maximum usage of nodes closer to the sink node. With this energy deployment, we maintained the same overall amount of energy deployment units, in the non-uniform

energy deployment. However, under our assumption, the energy consumption should be 100% before the sensor network runs out of energy and dies. In the uniform energy deployment scenario, the sensor network dies when only about 17.86% of the energy is consumed. Therefore, under non-uniform deployment, the efficiency of a sensor network's energy usage can be roughly 5:6 times compare to the uniform energy deployment. The efficiency can be measured by the total number of messages that can be delivered, or the lifetime of the sensor network under the same transmission frequency.

V. PERFORMANCE AND RESULTS

In order to measure the performance of the algorithm we use java, AWT, swings to design and describe the simulation and compare the energy graph of the nodes in the grid. As described in previous discussion both the energy optimization and security issues are resolved by using EOSER protocol in wireless sensor network.

The information enlisted in information table-1 is given in detail below:

Table 1: Network Information Table.

Node ID	Directions	Energy Levels in percentage	Generated Data (Encrypted)	Decrypted Data
N1	Upper	7.0%	Mc4q	0.0
N2	Upper	40.0%	Mc4q	0.0
N3	Upper	12.0%	Mcex4Ma	31.0
N4	Downward	70.9%	Mc4q	0.0
N5	Backward	100.0%	Mxma4	44.1
N6	Backward	100.0%	Mc4q	0.0
N7	Forward	45.0%	Mc4q	0.0
N8	Forward	56.0%	Mc4q	0.0
N9	Forward	80.0%	Mc4q	0.0
N10	Downward	100.0%	Mc4q	0.0

The energy level table consists of the node ID, direction, energy level, encrypted data, and decrypted data.
The node ID is a dynamic identification number assigned to each node in a grid to know the initialization of packet. The direction tab shows the direction taken by routing protocol to reach the destination. Here we use four directions the upward, downward, backwards and forward direction. Depending on situation the routing protocol uses the direction.

Initially it is assumed that all the nodes have the energy levels at 100% depending on the usage it get reduced to depict that energy level tab is used, hence the data is encrypted by using some encryption and decryption algorithms to provide security and confidentiality from hackers so the next tab is used as encryption and finally the decryption tab to decrypt the data. Considering two routing strategies one is deterministic routing and another one is random walk routing, in deterministic routing shortest path is searched to teach the destination and in the random walk routing a random node is selected to send data to the destination. Here in the simulation scenario the source location privacy is preserved in the random walk routing so it does not show the source node address, it forwards the data through intermediate node.

C. Energy Graph

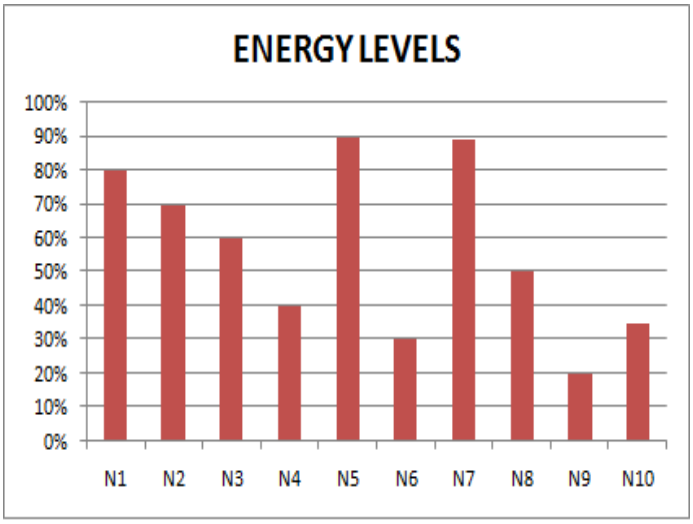

Fig -3 :shows remaining energy in each node.

The above graph shows the energy remaining in the each node. Here each node is named with node id N1,N2……Nn Depending on the number of node considered in wireless network and energy remaining is shown in each node.The protocol monitors the energy levels of each node in a network and selects the node close to the sink node and which is having highest level of energy and elect it as active node to increase the lifetime of the network.

VI. CONCLUSION

The Energy Optimized Secure Routing (EOSER) protocol for WSNs is proposed to balance the energy utilization and increase network lifetime. The energy balance consumption (EBC) and Probabilistic random Walk (PRW) strategies are used to module these proposed system. It has the flexibility to support multiple routing strategies in message forwarding to

extend the lifetime while increasing routing security. As we know that advancement in technologies is a never ending task, we may have further advancements in the energy calculations procedures and the algorithms used. Both theoretical analysis and experimental results show that EOSER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. It 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.

REFERENCES

[1] Di Tang, Tongtong Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE "Cost Aware Secure Routing (CASER)protocol design for wireless sensor network" IEEE Trans, Parallel Distribution system, vol. 26, no. 4, April 2015

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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 Proc. 19th Int. Conf. Comput. Commun.Netw., Aug. 2010, pp. 1–6.

[12] Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing," in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 88–93.

[13] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, Jun. 2009, pp.493–501.

[14] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., Mar. 15–19, 2010. pp. 1–9.

[15] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008, pp. 5155.

[16] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2005, pp. 599–608.

[17] Wikipedia Quartic function [Online]. Available: http://en.wikipedia.org/wiki/Quartic_function, Apr. 2014.

[18] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks :Attack and defense strategies," IEEE Netw., vol. 20, no. 3,pp. 41–47, May/Jun. 2006.

[19] Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: Issues and challenges," in Proc. 8th Int. Conf. Adv. Commun. Technol., 2006, pp. 1043–1048.

[20] 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.

[21] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in Proc.