Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.61 – 66

Secure and Efficient Energy-Aware Secure Routing (EASER) Protocol for Wireless Sensor Networks

MANJUNATH D R[1], Dr. THIMMARAJU S N[2]

[1]Research Scholar, Visvesvaraya Technological University, Belagavi, manjunathdrcs@gmail.com
[2]Professor, Dept. of Masters of Computer Applications, Visvesvaraya Technological University, Centre for Post Graduate Studies, Mysore l, thimmaraju_sn@yahoo.com

Abstract*—Over the last decade researchers has been a developing interest in domain of Wireless Sensor Networks (WSNs) due to numerous increasing automated industry and battle field applications. Minimizing energy expenditure and spreading WSN lifetime are prodigious tasks. Development of energy saving routing mechanism is one of the main issues in WSNs. There is a developing worry about security of information gained by effortlessly open remote sensors and these low power gadgets are not appropriate for complex cryptographic calculations. Henceforth, lifespan improvement and security are two clashing design issues for multi-hop remote sensor systems (WSNs) with non-replenishable energy assets. This paper proposes a protected and effective Energy-Aware Secure Routing (EASER) protocol to address these two clashing issues through two customizable parameters: energy balance mastery and probabilistic random walking. The convention finds that the energy utilization is seriously disproportional to the uniform energy deployment, which incredibly lessens the lifetime of the sensor systems, for the given network topology. An efficient non-uniform energy deployment strategy is designed to solve this problem under the similar security requirement and energy resource. Additionally proposed a quantitative security analysis to address the source location privacy. The protocol provides an excellent trade-off between energy balance and routing efficiency, and can also significantly extend the lifespan of the sensor networks in all situations. Further, the non-uniform energy deployment demonstrates that an expansion in the lifespan of the network and the total number of packets delivered. This paper presents analysis and simulation results in details to illustrate how different parameters act amongst energy efficiency and security.

***Keywords:* wireless sensor network, energy aware, secure routing protocol, lifetime optimization, energy consumption, uniform energy, deployment, strategy, security**

I. INTRODUCTION

WIRELESS sensor networks (WSNs) have turned into a pervasive answer for an extensive variety of utilizations. WSN is utilized to gather the crude information from harsh environment like health applications, natural climate, forests fire, military operation, volcanoes, home automation and many more. Sensor nodes are naturally equipped with energy constrained batteries, hence, it is vital important to design energy efficient protocols for them keeping in mind, the end goal to drag out their lifetime. Another extremely challenging design issue is routing for WSNs. An appropriately designed routing protocol not just guarantee low energy consumption and high message delivery ratio for message delivery, additionally also balance energy consumption of the entire wireless sensor network, and there by extend the sensor network lifespan.

Wireless sensor systems (WSNs) in fact and financially attainable to be generally utilized as a part of both military and nonmilitary personnel applications, for example, checking of encompassing conditions identified with the earth, valuable species and basic frameworks. A key component of such frameworks is that each system comprises of a substantial number of unattended sensor hubs. The steering is another extremely difficult plan issue for WSNs. A legitimately composed steering convention ought not just guarantee high message conveyance proportion and low vitality utilization for message conveyance, additionally adjust the whole remote sensor arrange vitality utilization, and there by develop the sensor organize lifetime. Persuaded by the way that WSNs routing is frequently topography based, this paper propose geology based secure and productive Energy-Aware secure routing (EASER) protocol for WSNs without depending on flooding. EASER permits messages to be transmitted using two routing methods, deterministic routing and random walking, in a similar structure. The appropriation of these two systems is controlled by the particular security necessities. EASER convention has two noteworthy focal points: (i) It ensures balanced essentialness usage of the entire remote sensor arrangement, so that the lifespan of the WSNs can be expanded, (ii) EASER convention supports various steering methodologies in light of the coordinating necessities, including brisk/direct message delivery and secure message movement to neutralize directing follow back assaults and noxious movement sticking assaults in WSNs.

We summarized our contribution as follows:

- We put forward an efficient Energy-aware secure routing protocol for WSNs. In this convention, energy-aware based routing plan activity can be connected to address the message delivery necessities.
- We think of the quantitative plan to steadiness the energy consumption in order to ensure that both the sensor network lifespan and to maximized the total number of messages that can be delivered underneath a similar energy deployment.
- We evolve theoretical formulas to estimate the number of routing hops in EASER under veering routing energy balance control and security prerequisites.
- We also analyze the security of suggesting routing algorithm and provides an ideal non-uniform energy deployment proposed action based largely on the energy consumption ratio for the given sensor networks.

Our both (theoretical and simulation) results demonstrate under the similar complete energy deployment.

II. Related Work

In WSN delay is the factor to some delay-sensitive applications, such as health or military applications. Many researchers have been proposed to achieve a good trade-off between power consumption and delay. Adaptive listening suggests the use of overhearing to reduce the sleep delay. In [1] authors proposes for a first time a secure and efficient Cost-Aware Routing (CASER) protocol that can address both energy balance and routing security concurrently in WSNs. In this protocol, each sensor node necessary to maintains the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using above information, each sensor node can create varying filters based on the expected design trade-off between security and efficiency. In [2] authors proposed an efficient source anonymous message authentication scheme (SAMA). SAMA can be applied to any messages to provide hop-by-hop message content authenticity while ensuring message sender privacy, without the weakness of the built-in threshold of the polynomial-based scheme. In [3] authors proposed a geographic adaptive fidelity (GAF) routing scheme. This routing scheme focuses on turning the radio off as much as possible, here the network area is divided into fixed size virtual grids. In every grid, only one node designated as the active node, while the others will sleep for an interval of time to save energy. Geographic routing leads to local minimum problem. In [1] discussed how greedy and face routing protocol combined to solve local minimum problem. In [6] gives the review about the QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks. QoS directing is a vital research issue in remote sensor systems (WSNs), particularly for mission-basic observing and observation frameworks which requires auspicious and dependable information conveyance. In [7] authors analyzed the source anonymity problem.

Source-location privacy is achieved through broadcasting valid messages that mixed with dummy messages. Here each node needs to transmit messages consistently that is at whatever time when there is no valid message to transmit; the node has to transmits dummy messages. The transmission of dummy messages leads to consumes notable amount of sensor energy and also increases the network collisions. In [8], [9], authors developed a two-phase routing algorithm to provide both source location privacy and confidentiality.

III. Proposed System

To overcome certain drawbacks and to improve efficiency we proposed enhanced scheme on CASER protocol and named as EASER. A secure and efficient Energy-aware Secure Routing (EASER) protocol is used to address energy balance and routing security concurrently in WSNs. In EASER routing protocol, each sensor node necessary to maintains the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using above information, each sensor node can create varying filters based on the expected design trade-off between efficiency and security. The security analysis clearly shows the proposed algorithm can protect the source location information from the attackers.

With the above assumptions, the proposed algorithm can be put into the following modules.

- Network Creation
- Energy Balance Control
- Secure Approach for Routing

A. Network Creation

In this module the WSN is formed which composed of a large number of sensor nodes and a sink node. 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 available to public. The network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node with the highest energy level in each grid is selected as the active head node for message forwarding. Every node in the grid will maintain it's certain attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighboring grids. The information maintained by each sensor node will be updated periodically. The information about the relative location of the sensor domain may be broadcasted in the network to update routing information.

B. Energy Balance Control

This Module presents the neighbouring node selection; the energy level of each node to be considered. To achieve the energy balance, monitor and control the energy consumption for the nodes with relatively low energy levels. To select the grids with relatively higher remaining energy levels for message forwarding. For parameter to enforce the degree of the energy balance control. It can be easily seen that a larger a corresponds to a better EBC. It is also clear that increasing of a main they also increase the routing length it can effectively control energy consumption from the nodes with energy levels lower than Node *A*. For node *A*, N_A denoted as the set of its immediate adjacent neighboring grids and the remaining available energy of grid *i* as ε_{r_i} , $i \in N_A$. The EASER path selection algorithm is derivate by the equation,

$$\varepsilon_\alpha(A) = \frac{1}{|N_A|} \sum_{i \in N_A} \varepsilon_{r_i}$$

Using the above equation node *A* can compute the average available remaining energy of the grids N_A. To balance energy among all the grids in WSN we introduce a parameter α∈ [0, 1], so that for message forwarding we configuring *A* to only select the grids with comparatively higher remaining energy levels.

C. Security Approach for Routing

In the proposed demonstrate the information that is transmitted by the steering system. A directing methodology that can give steering way eccentrics and security. The steering way turns out to be more variable. The directing convention contains two alternatives for message sending: one is a deterministic most limited way directing framework determination calculation, and the other is a safe steering matrix choice calculation through arbitrary strolling. In the deterministic steering approach, the next node is chosen from

N_A^α in light of the relative areas of the grids. For message forwarding the grid which is nearest to the sink node is chosen. In the safe steering case, the next hop grid is arbitrarily chosen from N_A^α for message forward.

The dissemination of these two calculations is controlled by a security level called *β∈ [0, 1]*, conveyed in each message. At the point when a node needs to advances message, the node first chooses an arbitrary number *γ∈ [0,1]* If *γ>β* , then the node chooses the following hop grid on basis of shortest path routing algorithm; elsewise random walking scheme is used to choose the next hop grid. The security level *β* is a customizable parameter. A littler *β* brings about a shorter routing way and also energy efficient in message forwarding.

EASER ALGORITHM

```
Step 1: At source node, create DATA packets:
        ➢ Given the value of 'alpha'
        ➢ Set the value of 'beta' for every node:
        ➢ Calculate threshold Energy = alpha * average Energy;

Step 2: Chose a random number for the value of 'gamma'
    if (gamma > beta) then
        ➢ Select a grid whose remaining average energy is more
          and greater than threshold energy.
        ➢ Select a shortest node to the sink node from selected grid
        ➢ Send the packet to the selected node.
    else
        ➢ Choose a random node from the neighbor node set and
        send to it.
    end if
```

IV. ALGORITHM

The energy Balance Control algorithm shows, pointed out that the EBC parameter can be configured in the message level, or in the node level based on the application scenario and the preference. When α increases from 0 to 1, more and more sensor nodes with relatively low energy levels will be excluded from the active routing selection. Therefore, the N_A^α shrinks as α increase. In other words, as *α* increase, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since *ε∈ (A)* is defined as the average energy level of the nodes in N_A,this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from N_A^α .

At the point when β increases random walking scheme is used to select next hop grid. In like manner, the directing way turns out to be more arbitrary. At the point when b < 1, since EASER blends random walking scheme with deterministic shortest path routing ensures that the messages are sent from the source node to the sink node. In any case, the steering way turns out to be more dynamic and eccentric. Along these lines, it is more troublesome for the foe to catch the message or to stick the activity. Hence, the conveyance proportion can be expanded in a threatening domain. While giving steering security, directing bounce separate increments with the security level β.

V. PERFORMANCE ANALYSIS

The EASER protocol provides the network lifetime and increasing the security for wireless sensor networks. Fig 5.1 network lifetime .The Fig 5.2 shows that, a x graph is plotted for network life time. X-axis denotes the number of nodes and Y-axis denotes the energy level (J). The energy level unit is joule. Compare to the existing system proposed system network lifetime is increasing. Red color line denotes the increasing energy and green color line denotes the delivery ratio for energy.

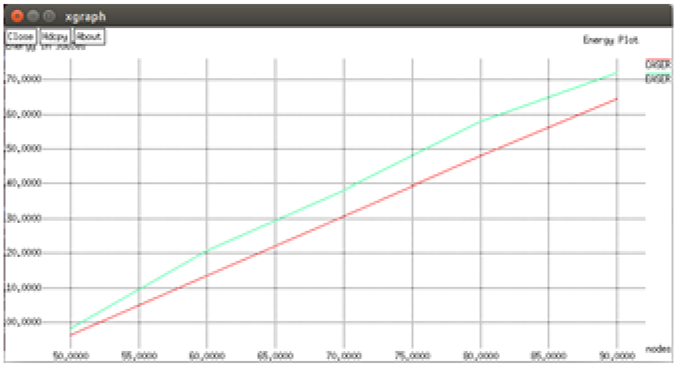

Fig 5.1 Energy of the network v/s number of nodes

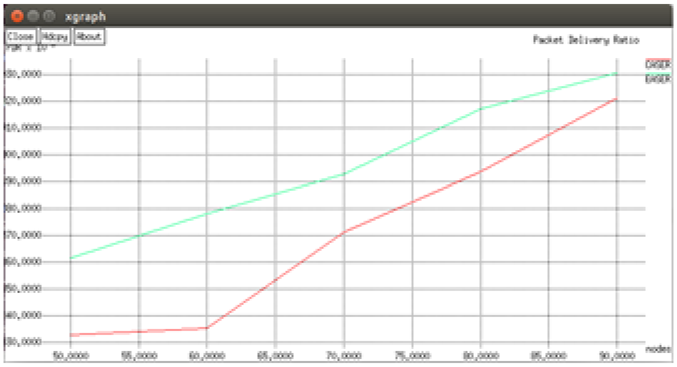

Fig 5.2 Packet delivery ratio v/s number of nodes

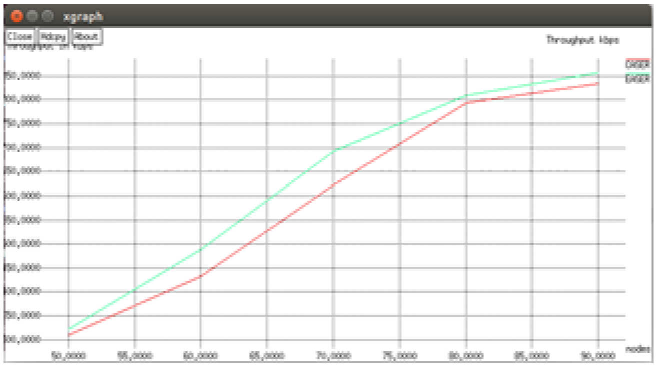

Fig 5.3 Throughput of the network v/s number of nodes.

VI. Conclusion

This Paper presents enhanced secure and energy efficient protocol based on Energy-aware secure Routing (EASER) protocol for WSNs to balance the energy consumption in non- uniform energy deployment strategy and increase network lifespan. For message forwarding, this protocol is support multiple routing to extend the lifespan and increasing routing security. Our theoretical analysis and simulation results both provide that EASER has an excellent routing performance in terms of routing path security and energy balance.

References

[1] Di Tang, Tongtong Li, Jian Ren, "Energy-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks" IEEE Trans.on Paral. Dist. Syst. 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 Distributed. 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. Computing. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

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

[5] Long Cheng, Jianwei Niu, Jiannong Cao "QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed System, Volume: 25, Issue: 7, July 2014 ,pages: 1864 - 1875.

[6] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE 27th Conference. Computing. Communication, Apr. 2008, pages. 51–55.

[7] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proc. IEEE 6th Annual. Communication. Soc. Conference .Sens., Mesh Ad Hoc Communication. Networks. Rome, Italy, Jun. 2009, pp.493–501.

[8] 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.

[9] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annual. International. Conf. Mobile Computing. Networks., Jul. 2001, pages. 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 Computing. Commun., 1999, pp. 48–55.

[11] Rupinder Singh,, Dr. Jatinder Singh,, and Dr. Ravinder Singh, "Security Challenges in wireless nsensor networks" International Journal of Computer Science and Information Technology & Security ISSN: 2249-9555 Vol.6, No3, May-June 2016

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

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

[14] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. IEEE Wireless Commun. Networking. Conf., Mar. 17–21, 2002, vol. 1, pp. 350–355.K. Chen, *Linear Networks and Systems*. Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.