International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

An Efficient Cost-A ware Secure Routing (CASER) Protocol for Wireless Sensor Network

[1] R. Rajeshwari [2] R.Arul Jothi [3] S.Bhuvaneswari [4] P. Jayamary Fathima [5] A.Ajin Brabasher M.E.,
[1][2][3][4] UG student, [5] Assistant Professor
Department of CSE, Loyola Institute of Technology, Chennai, India.
[1] rajilal96@gmail.com [2] r.jothi25@gmail.com [3] sbhuvaneswari187@gmail.com
[4] jayamaryfathima@gmail.com[5] ajinbrabasher04@gmail.com

***Abstract* — It is well known that wireless sensor networks (WSNs) is a self-organization wireless network system constituted by numbers of energy-limited micro sensors under the banner of industrial application (IA). In this project, we propose a secure and efficient Cost Aware Secure Routing (CASER) protocol to address two conflicting issues; They are lifetime optimization and security. Through the energy balance control and random walking, we can address those conflicting issues. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. 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.**

Index Terms: Wireless Sensor Network (WSN), Cost Aware SEcure Routing(CASER) Protocol, Security, Lifetime optimization, Energy deployment.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator used to monitor the physical, environment all quantity such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. we propose a 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. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. In addition, we also give quantitative secure analysis on the proposed routing protocol based on the criteria proposed in,

CASER protocol has two major advantages:
It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.
CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing trace back attacks and malicious traffic jamming attacks in WSNs.

II. MAIN CONTRIBUTIONS:

Our contributions of this paper can be summarized as follows:

- 1)We propose a secure and efficient Cost Aware SEcure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based routing strategies can be applied to address the message delivery requirements.
- 2)A quantitative scheme to balance energy so that both the sensor network lifetime and the total number of messages can be delivered are maximized under the same energy deployment
- 3) We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.
- 4)We quantitatively analyze security of the proposed routing algorithm.
- 5)We provide an optimal non-uniform energy deployment (noED) strategy for the given sensor networks based on the energy consumption ratio. Our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

III. RELATED WORK

Routing is a challenging task in WSNs due to the limited resources .Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination. The source chooses the immediate neighboring node to forward the message based on either the direction or the distance. The distance between the neighboring nodes can be estimated or acquired by signal strengths or using GPS equipments. The relative location information of neighbor nodes can be exchanged between neighboring nodes.

In, 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 fixed size virtual grids. In each grid, only one node is selected as the active node, while the others will sleep for a period to save energy. The sensor forwards the messages based on greedy geographic routing strategy. A query based geographic and energy aware routing (GEAR) was propose. In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighboring nodes based on estimated cost Aware SEcure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based routing strategies can be applied to address the message delivery requirements

2)A quantitative scheme to balance energy so that both the sensor network lifetime and the total number of messages can be delivered are maximized under the same energy deployment

3) We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.

4)We quantitatively analyze security of the proposed routing algorithm.

5)We provide an optimal non-uniform energy deployment (noED) strategy for the given sensor networks based on the energy consumption ratio. Our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario and learning cost. The estimated cost considers both the distance to the destination and the remaining energy of the sensor nodes. While the learning cost provides the updating information to deal with the local minimum problem.

While geographic routing algorithms have the advantages that each node only needs to maintain its neighboring information, and provides a higher efficiency and a better scalability for large scale WSNs, these algorithms may reach local minimum, which can result in dead end or loops. To solve the local minimum problem, some variations of these basic routing algorithms were proposed in, including GEDIR, MFR and compass routing algorithm. The delivery ratio can be improved if each node is aware of its two-hop neighbors. There are a few papers discussed combining greedy and face routing to solve the local minimum problem. The basic idea is to set the local topology of the network as a planar graph, and then the relay nodes try to forward messages along one or possibly a sequence of adjacent faces toward the destination.

Lifetime is another area that has been extensively studied in WSNs. In ,a routing scheme was proposed to find the sub-optimal path that can extend the lifetime of the WSNs instead of always selecting the lowest energy path. In the proposed scheme, multiple routing paths is set ahead by a reactive protocol such as AODV or directed diffusion. Then, the routing scheme will choose a path based on a probabilistic method according to the remaining energy. In, Chang and Tassiulas assumed that the transmitter power level can be adjusted according to the distance between the transmitter and the receiver. Routing was formulated as a linear programming problem of neighboring node selection to maximize the network life- time .Then Zhang and Shen investigated the unbalanced energy consumption for uniformly deployed data- gathering sensor networks. In this paper, the network is divided into multiple corona zones and each node can per- form data aggregation. To the best of our knowledge, none of these schemes have considered privacy from a cost- aware perspective.

In this paper, for the first time, 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 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. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. Our extensive OPNET simulation results show that CASER can provide excellent energy balance and routing security. It is also demonstrated that the proposed secure routing can increase the message delivery ratio due to reduced dead ends and loops in message forward.

IV. MODLES:

A. *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

2.2 DESIGN GOALS:

Our design goal can be summarized as follows: To maximize the sensor network lifetime ,we ensure that the energy consumption of all sensor grids are balanced.

To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.

The adversaries should not be able to get the source location information by analyzing the traffic pattern.

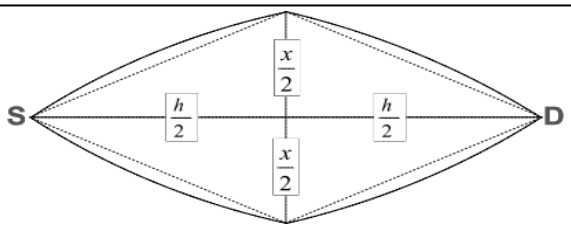
• The adversaries should not be able to get the source location information if he is only able to monitor a certain area of the WSN and compromise a few sensor nodes.

• 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.

• 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.

.

Routing paths



V. THE PROPOSED CASER ROUTING PROTOCOL:

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 that can balance energy consumption.

a. 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 ∑ ; i 2 N A. With this information, the node A can compute the average remaining energy of the grids in N A as

$$\in (A) = \frac{1}{|Na|\sum i} \in Naeri$$

N A Eri. 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. For this purpose, we introduce a paramete0r to enforce the degree of the energy balance control.

b. Secure Routing Strategy:

In the previous section, we only described the shortest path routing grid selection strategy. However, in CASER protocol, we can support other routing strategies. In this section, we propose a routing strategy that can provide routing path unpredictability and security. The routing protocol contains two options for message forwarding: one is a deterministic shortest path routing grid selection algorithm, and the other is a secure routing grid selection algorithm through random walking.

c. CASER Algorithm:

• 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.

• 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.

THEOREM 2.

Assume that the network is randomly deployed and each sensor node is initially deployed with equal initial energy. We also assume that data generation in each sensor node is a random variable. Then for a given routing cost factor f, the optimal security level can be estimated from the following quartic equation:

$4f^2x^4 - 5x^2 + 2x - 1 = 0$

Where $x = 1 - \beta$

Proof: According to Corollary 2, we have

$\sqrt{\left[1 + \left(\frac{\beta}{2(1-\beta)}\right)\right]^2}$ /1-β

Multiply both sides with 1-β, we have

$\sqrt{\left[1 + \left(\frac{\beta}{2(1-\beta)}\right)\right]}$ ^2=f (1-β)

Square of both sides, we get

$\left(1 + \left(\frac{\beta}{2(1-\beta)}\right)\right)$^2=$f^2$ (1-β)^2

Equivalently, we have

4(1-β)^2+ $\beta^2 = 4(1-\beta)$^4

Let$(1-\beta) = x$ we can derive

$\beta^2 = (1-x)^2 = x^2 - 2x + 1$,

reorganize the above Equation, we get

$4f^2x^4 - 5x^2 + 2x - 1 = 0$

Equation can be solved using Ferrari's method following Algorithm 3 to recover

$s = 1 - \beta$.

The security level b can be recovered as :

$\beta = 1 - s$.

VI. SECURITY ANALYSIS

In CASER, the next hop grid is selected based on one of the two routing strategies: shortest path routing or random walking. The selection of these two routing strategies is probabilistically controlled by the security level b. The security level of each message can be determined by the message source according to the message priority or delivery preference. As b increases, the routing path becomes more random, unpredictable, robust to hostile detection, immune to interception and interference attacks. While random walking can provide good routing path unpredictability, it has poor routing performance. CASER provides an excellent balance between routing security and efficiency.

***a. Quantitative Security Analysis of CASER*:**

we introduced criteria to quantitatively measure source-location privacy for WSNs.

Definition1*:* (Source-location Disclosure Index). SDI measures, from an information entropy point of view, the amount of source-location information that one message can leak to the adversaries.For a routing scheme, to achieve good source-location privacy, SDI value for the scheme should be as close to zero possible.

Definition 2: (Source-location Space Index) SSI is defined as the set of possible network nodes, or area of the possible network domain, that a message can be transmitted from.

For a source-location privacy scheme, SSI should be as large as possible so that the complexity for an adversary to perform an exhaustive search of the message source is maximized.

Definition 3: (Normalized Source-location Space Index (NSSI)).

NSSI is defined as the ratio of the SSI area over the total area of the network domain. The d is called the local degree. Based on these criteria, we can evaluate security of the CASER routing protocol.

***b. Dynamic Routing and Jamming Attacks*:**

For security level b, the distribution between random walking and the shortest path routing for the next routing hop is β and 1- β. β can vary for each message from the same source. In this way, the routing path becomes dynamic and unpredictable. In addition, when an adversary receives a message, he is, at most based on our assumption, able to trace back to the immediate source node that the message was transmitted. Since the message can be sent to the previous node by either of the routing strategies, it is infeasible for the adversary to determine the routing strategy and find out the previous nodes in the routing path.

The CASER routing algorithm distribute the routing paths in a large area based on our above analysis due to the random and independent routing selection strategy in each forwarding node. This makes the likelihood for multiple messages to be routed to the sink node through the same routing path very low even for the smart jammers that have knowledge of the routing algorithm.

c. Energy Level and Compromised Node Detection:

Since we assume that each node has knowledge of energy levels of its adjacent neighboring grids, each sensor node can update the energy levels based on the detected energy usage. The actual energy is updated periodically. For WSNs with non replenishable energy resources, the energy level is a monotonically decreasing function. The updated energy level should never be higher than the predicated energy level since the predicted energy level is calculated based on only the actually detected usage. If the updated energy level is higher than the predicted level, the node must have been compromised and should be excluded from its list of the adjacent neighboring grids.

VII. PERFORMANCE EVALUATION AND SIMULATION RESULTS:

In this section, we will analyze the routing performance of the proposed CASER protocol from four different areas: routing path length, energy balance, the number of messages that can be delivered and the delivery ratio under the same

energy consumption. Our simulations were conducted in a targeted sensor area of size 1500 * 1500 meters divided into grids of 15* 15.

***a. Routing Efficiency and Delay*:**

For routing efficiency, we conduct simulations of the proposed CASER protocol using OPNET to measure the average number of routing hops for four different security levels. We randomly deployed 1,000 sensor nodes in the entire sensor domain. We also assume that the source node and destination node are 10 hops away in direct distance. The routing hops increase as the number of transmitted messages increase. The routing hops also increase with the security levels.

***b. Energy Balance*:**

The CASER algorithm is designed to balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels. In this way, we can extend the lifetime of the sensor networks. Through the EBC a, energy consumption from the sensor nodes with relatively lower energy levels can be regulated and controlled. Therefore, we can effectively prevent any major sections of the sensor domain from completely running out of energy and becoming unavailable.

In the CASER scheme, the parameter a can be adjusted to achieve the expected efficiency. As a increases, better energy balance can be achieved. Meanwhile, the average number of routing hops may also increase. Accordingly, the overall energy consumption may go up.

c. Delivery Ratio:

One of the major differences between our proposed CASER routing protocol and the existing routing schemes is that we try to avoid having any sensor nodes run out of energy while the energy levels of other sensor nodes in that area are still high. We implement this by enforcing a balanced energy consumption for all sensor nodes so that all sensor nodes will run out of energy at about the same time. This design guarantees a high message delivery ratio until energy runs out from all available sensor nodes at about the same time. Then the delivery ratio drops sharply.

VIII. CONCLUSIONS

In this paper, we presented a secure and efficient Cost Aware SEcure Routing (CASER) protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to exten00000000d the lifetime while increasing routing security. Both theoretical analysis and simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We 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.

REFERENCE

[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.sHeidemann, 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, TTR-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.

[16] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2258–2267, Jul. 2010.

[17] 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.

[18] C. 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. [19] 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.

[20] 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.

[21] 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. 51–55.

[22] 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.

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

[24] 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.

[25] A. 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.