International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Energy Efficient Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks

BHADHAVATH RATHNA SREE
ASSISTANT PROFESSOR IN DEPT. OF CSE
UNIVERSITY COLLEGE OF ENGINEERING AND TECHNOLOGY, MAHATMA GANDHI UNIVERSITY, NALGONDA, TS.
badavathrathnasree@gmail.com

Abstract— Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) In this paper, I first propose a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking .Then determine 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, I propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. Also provide a quantitative security analysis on the proposed routing protocol. For the non-uniform energy deployment, our analysis shows that I can increase the lifetime and the total number of messages that can be delivered under the same hypothesis. And also propose sleep awake state algorithms for achieve a high message delivery ratio while preventing routing blocking attacks.

Keywords— Message Delivery ratio, lifetime ***energy, preventing attacks***

I. INTRODUCTION

Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure a 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, 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.

This scenario is analogous to delivering US Mail through USPS: express mails cost more than regular mails; however, mails can be delivered faster. 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.

The rest of this paper is organized as follows. In Section II, the related work is reviewed. The proposed scheme is described in Section III. In Section IV provides performance analysis of the proposed scheme. We present the optimal, non-uniform energy deployment strategy for CASER in Section V. We conclude in Section VI.

II. RELATED WORK

Routing is a challenging task in WSNs due to the limited resources. Geographic routing has been widely viewed as one of the most promising approaches for WSNs. Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination.

While geographic routing algorithms have the advantages that each node only needs to maintain its neighboring information, and provide a higher efficiency and a better scalability for large scale WSNs, these algorithms may reach their 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, source-location privacy is provided through broadcasting that mixes valid messages with dummy messages. The main idea is that each node needs to transmit messages consistently. Whenever there is no valid message to transmit, the node transmits dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the network collisions and decreases the packet delivery ratio.

The (SEEM) routing protocol has three types of nodes such as sensor node, sink node and base station node. The base station plays an important role in finding multiple paths between the source and the sink node. The control overhead is very high in the SEEM model as it uses Neighbour Discovery (ND) packet, Neighbour Collection (NC) packet and Neighbour Collection Reply (NCR) packet in the routing protocol. The ND packet is broadcast in network to know the neighbouring nodes of every node. Once all the nodes identify their neighbouring nodes, the base station node broadcasts NC packets in order to collect the neighbour's information of each node gathered during the previous broadcasting. The sensor nodes acknowledge to the NC packet by sending the neighbour collection reply packet to the base station. They SEEM model justifies the security without using the crypto system mechanism in the routing protocol.

III. PROPOSED SCHEME

This paper proposes 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 neighbouring 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 -justified.

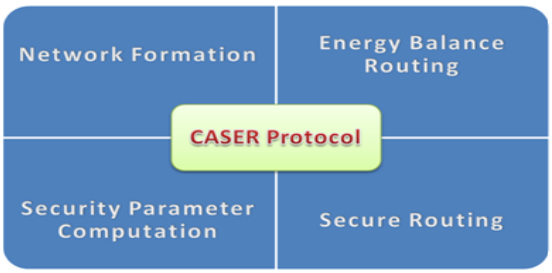

Fig 1. Architecture of CASER Protocol

1. Network formation

In this module the network is formed for secure routing. The networks are composed of a large number of sensor nodes and a sink node. Each sensor node has a very limited and non-replenish able energy resource. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy.

The network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node for message forwarding.

Each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids. The information maintained by each sensor node will be updated periodically.

2. Energy Balance Routing

This module send message from sensor to sink using EBC (Energy Balance Control) parameter [0, 1]. 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 NA and the remaining energy of grid i as Eri , i NA. With this information, the node A can compute the average remaining energy of the grids in NA as Ea(A) = 1/NA I NA Eri..

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 candidate set for the next hop node as N A={i NA | Eri Ea(A)} based on the EBC. Increasing of a may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than Ea(A).

3. Security Parameter Computation

This module computes security parameter for secure routing using cost factor f. This security parameter is used to find the maximum routing security level. The following steps are used to compute

1. $a \leftarrow 4f^2; c \leftarrow -5; e \leftarrow -1;$
2. $A \leftarrow \frac{c}{a}; B \leftarrow \frac{d}{a}; C \leftarrow \frac{e}{a};$
3. $p \leftarrow -\frac{1}{12}A^2 - C; q \leftarrow -\frac{A^3}{108} + \frac{AC}{3} - \frac{B^2}{8};$
4. $r \leftarrow -\frac{q}{} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}};$
5. $u \leftarrow \sqrt[3]{r};$
6. $y \leftarrow -\frac{5}{6}A + u - \frac{p}{3u}; w \leftarrow \sqrt{A + 2y};$
7. $s \leftarrow \frac{-w + \sqrt{-3A + 2y + 2B/w}}{2};$
8. $\beta \leftarrow 1 - s$

4. Caser Routing

This module provides 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.

In the deterministic routing approach, the next hop grid is selected from NA based on the relative locations of the grids. The grid that is closest to the sink node is selected for message forwarding. In the secure routing case, the next hop grid is randomly selected from NA for message forwarding. The distribution of these two algorithms is controlled by a security level called [0, 1] carried in each message.

IV. PERFORMANCE EVALUATION AND SIMULATION RESULTS

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.

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 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.

V. NON-UNIFORM ENERGY DEPLOYMENT STRATEGY FOR CASER

We can see that the message delivery ratio drops as $ increases. This is because the overall energy consumption increases as the required security level increases. We also found that under the proposed CASER protocol, non-uniform energy deployment can increase the energy efficiency and network lifetime even when security is required in WSNs.

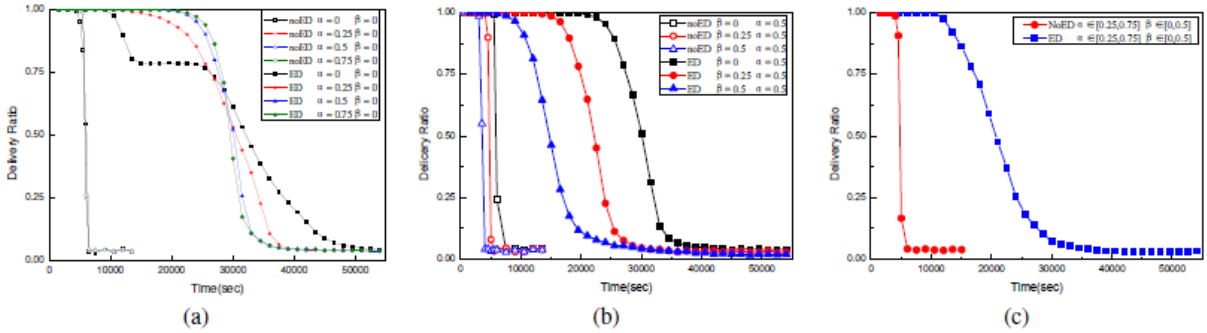

Fig. 2 Message delivery ratio: (a) $\beta = 0$ and varying α, (b) $\alpha = 0.5$ and varying β, (c) varying α and β, where $\alpha \in [0.25, 0.75], \beta \in [0, 0.5]$

VI. CONCLUSION

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 extend 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.

REFERENCES

[1] S. Y. Li, J. Ren, and J. Wu, —*Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,"* IEEE Transactions on Parallel and Distributed Systems, accepted, to appear.

[2] J Y. Li, J. Li, J. Ren, and J. Wu, —*Providing hop-by-hop authentication and source privacy in wireless sensor networks*,‖ in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012 2012.

[3] S B. Karp and H. T. Kung, —*GPSR: Greedy perimeter stateless routing for wireless networks*,‖ in MobiCom'2000, New York, NY, USA, 2000, pp.243 – 254..

[4] J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, —*Ascalable location service fo geographic ad hoc routing,"* in MobiCom'2000.

[5] Y. Xu, J. Heidemann, and D. Estrin, —*Geography-informed energy conservation for ad-hoc routing*,‖ in the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001, pp. 70–84 (2002)

[6] Y. Yu, R. Govindan, and D. Estrin, ―*Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks*,‖ UCLA Computer Science Department Technical Report, UCLACSD, May 2001

[7] ―N Bulusu, J. Heidemann, and D. Estrin, ―*Gps-less low cost outdoor localization for very small devices,"* Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, ―*Dynamic fine-grained localization in ad-hoc networks of sensors,"* in Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom), July 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, ―*Routing with guaranteed delivery in adhoc wireless networks*,‖ in 3rd Int. Workshopon Discrete Algorithms and methods for mobile computing and communications,

[10] [10] ——, ―*Routing with guaranteed delivery in ad hoc wireless networks,"* in the 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL M 99), Seattle, WA, August 1999, pp. 48–55.