© 2017 IJSRST | Volume 3 | Issue 4 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Cost Aware Secure Network Protocol Design for Wireless Sensor Network

Rozeena S. Sheikh[1], S. Sahare[2], A. Manusmare[3]

[1]M.Tech Student, Department of Electronics & Communication Engineering, Ballarpur Institute of Technology, Chandrapur, Maharashtra, India
[2]Professor, Department of Electronics & Communication Engineering, Ballarpur Institute of Technology, Chandrapur, Maharashtra, India
[3]Professor, Department of Electronics & Communication Engineering, Ballarpur Institute of Technology, Chandrapur, Maharashtra, India

ABSTRACT

This paper concerns with Sensor networks which are a prominent representative of fastest computing technologies. The limited resources of sensor nodes and the low reliability of wireless communication pose special challenges for message routing in sensor networks. This paper gives context awareness can enhance routing in sensor networks. Further, we analyze the network properties which influence the benefit of context awareness in the routing process. The presented simulation results allow assessing which networks are best suited for such an approach.

Keywords: Routing, Security, Energy Efficiency, Energy Balance, Delivery Ratio, Deployment

I. INTRODUCTION

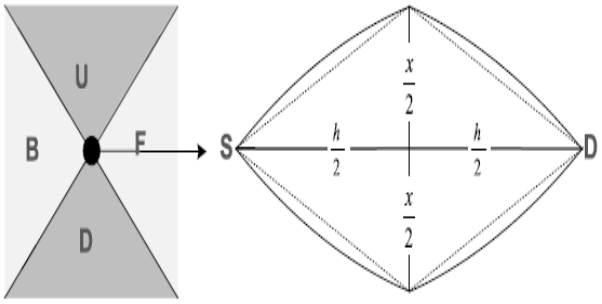
In recent years, the researches on effective use of wireless sensor (WSNs) which are feasible and widely used in most of the commercial and civilian application. Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. [1].

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. CASER protocol has two major advantages: (i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing traceback attacks and malicious traffic jamming attacks in WSNs.
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) We devise a quantitative scheme to balance the energy consumption so that both the sensor network.

II. PROPOSED WORK

Assuming that 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. 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.

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) Next hop node distribution (b) Routing path

Fig. 1. Routing path and length estimation.

In the CASER protocol, we assume that each node maintains its relative location and the remaining energy levels of its immediate adjacent neighboring grids. In the multi-hop routing protocol, node A selects its next hop grid only from the set NA 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 parameter $\alpha \in [0,1]$ to enforce the degree of the energy balance control. We define the candidate set for the next hop node $N_A^{\propto} = \{i \in N_A \, | \varepsilon_{ri} \geq \propto \varepsilon_a (A)\}$ based on the EBC $\propto$. It can be easily seen that larger $\propto$ corresponds to a better EBC. It is also clear that increasing of a may also increase the routing length. However, it can effectively control energy consumption from the nodes with energy levels lower than $\propto \varepsilon_a (A)$. Let, summarize the CASER routing protocol in Algorithm 1. It should be pointed out that the EBC parameter a can be configured in the message level, or in the node level based on the application scenario and the preference. When a 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 $N_A^{\propto}$ shrinks as $\propto$ increases In other words, as $\propto$ increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since $\varepsilon_a (A)$ is defined as the average energy level of the nodes in NA, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from $N_A^{\propto}$.

Algorithm 1

Node A finds the hop routing grid based on the EBC $\alpha \in [0,1]$.

1. Compute the average remaining energy of theadjacent neighboring grid.

$\varepsilon_a (= \quad = \frac{1}{NA} \sum_{i \varepsilon NA}$

2. determine the candidate grid for the next routing hop:

$N_A^{\propto} = i \in | \quad \geq \propto \varepsilon_a$ (send the message in the Grid in the $N_A^{\propto}$ that is closest to sink node based on its relative based on its relative location.

A. Secure Routing Strategy

In this we follow only the shortest path routing grid selection strategy 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.

TABLE 1.routing HOPS for different EBC parameter.

$\mu' = 200, \sigma' = 50$

EBC parameter	Average hops in simulations	Estimated CASER hops
0	10	10
0.1	10.26	10.05
0.2	10.38	10.09
0.3	10.63	10.18
0.4	11.02	10.34
0.5	11.15	10.64

When a node needs to forward a message, the node first Selects a random number $\gamma \in (0,1)$. If $\gamma > \beta$ then the node selects the next hop grid based on the shortest routing algorithm; otherwise, the next hop grid is selected using random walking. The security level β is an adjustable parameter. A smaller β results in a shorter routing path

and is more energy efficient in message forwarding. On the other hand, a larger b provides more routing diversity and security.

B. Caser Algorithm

Based on the previous description, the CASER algorithm can be described in Algorithm 2. While providing routing path security, security routing will add extra routing over head due to the extended routing path.

Algorithm 2

Node A finds the hop routing grid based on the given parameter $\alpha, \beta \epsilon(0,$

1. Compute the average remaining energy of the adjacent neighboring grid.
   $\varepsilon_a (= \quad = \frac{1}{NA}\sum_{i\varepsilon NA}$
2. determine the candidate grid for the next routing hop:
   $N_A^{\propto} = i \in | \quad \geq \propto \varepsilon_a (.$
3. Select the random number $\gamma \epsilon (0$
4. If $\gamma \geq$ then send message to the grid in the l closest to the sink node based on its relative location.
5. Else route the message to randomly selected grid in the set l

C. Determine Security Level Based On Cost Factor

For a given routing budget, we can also find maximum routing security level. This result given in the following theorem:

Theorem:

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, the optimal security level can be estimated from the following quadratic equation:$4fx^4 - 5x^2 + 2x - 1 = 0$, where $x = 1 - \beta$

Above equation can be solved by using Ferrari's method.

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 β 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.

1) 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.

2) Energy Balance

The CASER algorithm is designed to balance the overall lsensor 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.

Table 2: Delay Results for various Security Parameter for Simulation

Security Parameter	0	0.125	0.25	0.375	0.5
Average Delay (Sec)	0.0148	0.0177	0.0214	0.0265	0.0344

III. RESULT

Provides the message delivery ratio in a more realistic scenario. Since the different messages may have different importance, we select both security parameters and energy balance levels randomly for non-uniform and uniform energy deployment in this simulation. The results demonstrate that non-uniform energy deployment can achieve a much higher delivery ratio while extending the lifetime of the WSN. To investigate the energy consumption in the uniform energy deployment, we assume each sensor node has equal probability to

generate packets and acts as a source node . In these simulations, the sink node is located in the center of the target area located at (750, 750), which makes the target area symmetrical to show the energy consumption. Each node has the same probability to generate the packets. The maximum direct distance between the source node and sink is 7. Similar to the previous simulation, we assume there are three nodes in each grid, and each node is deployed with energy to transmit 70 messages.

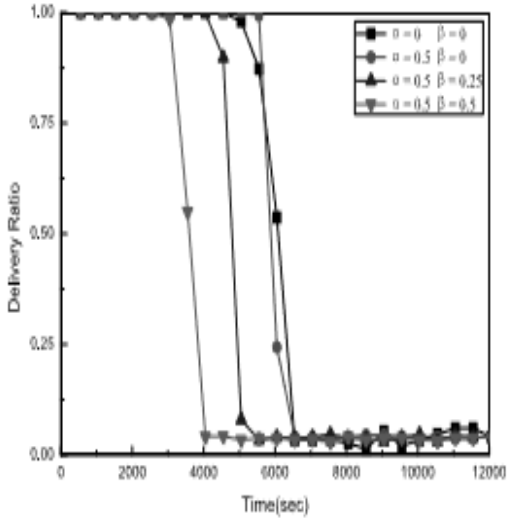


Fig: 2: Delivery Ration

IV. CONCLUSION & FUTURE SCOPE

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.

The future research for routing protocols in CR networks includes cross-layer design.. The cross-design needs the cooperation between routing and spectrum management functions in order to resourcefully become accustomed to modifications network properties. Also, there is strong need of a routing protocol for CR scenario which would be able to offer a better route selection. One of the open issues for routing protocols for CRASNs is the security aspect as the basic nature of CR networks makes them more vulnerable to attacks. An attacker node may deliberately block the available space in the spectrum resulting in degrading the performance of the system and also adversely affect the quality of service. We consider that critics on the existing routing protocols for CRAHNs is open up new emergent issues. In order to extend these already existing routing protocols or developing new routing scheme, their performance assessment needs to be done in real world scenario.

V. 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. 00729, Apr. 2000.