ANALYSIS ON WIRELESS SENSOR NETWORKS' COST AWARE SECURE ROUTING (CASER) PROTOCOL DESIGN

[1]G Shekar, [2]Boddupalli Santhosh, [3]T Radhika, [4]P Ramya
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Computer Science and Engineering, Brilliant Institute of Engineering and Technology, Hyderabad, India.

ABSTRACT

To monitor physical or environmental factors like temperature, noise, pressure, etc., wireless sensor networks of widely dispersed autonomous sensors are used. The sensors cooperatively communicate their data across the network to a central point. The CASER protocol is used to extend the network's life. The two competing concerns in WSN are energy consumption and security. Several factors are utilized to solve this issue. Particle swarm optimization (PSO) and lifetime optimization TORA are used to regulate the energy balance (Temporally ordered Routing Algorithm). For protection the proposed approach uses probabilistic random walking to achieve high message delivery rates while shielding routing against damaging assaults.

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

I. INTRODUCTION

Being a significant new layer in the IT ecosystem, Wireless Sensor Networks (WSN) are also a rich area of ongoing research encompassing hardware and system design, networking, distributed algorithms, programming models, data management, security, and social considerations. The fundamental concept behind a sensor network is to disseminate tiny sensing devices—capable of detecting changes in situations or characteristics and corresponding with other devices—across a defined geographic region for a defined purpose. like target tracking, watching over, keeping an eye on the environment, etc. Today's sensors may measure a variety of circumstances, including temperature, pressure, humidity, soil composition, vehicle movement, noise levels, illumination, the presence or absence of certain objects or substances, the mechanical stress on connected objects, and other factors. Another extremely difficult design problem for WSNs is routing. A properly 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 consumption, and thereby extend the sensor network lifetime. Motivated by the fact that WSNs routing is often 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. 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

EXISTING SYSTEM

In existing system geographic routing is used as the promising solution in the network. Geographic adaptive fidelity is used as the promising solution for the low power sensor network .A query based geographic and energy aware routing was implemented for the dissemination of the node. In Geographic and energy aware routing (Gear), the sink disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighboring nodes based on the estimated cost and the learning cost. Source-location privacy is provided through broadcasting that mixes valid messages not only consumes significant amount of sensor energy. But also increases the network collisions and decreases the packet delivery ration. In phantom routing protocol each message is routed from the actual source to a phantom source along a designed directed walk through either sector based approach or hop based approach. The direction sector information is stored in the header of the message. In this way, the phantom source can be away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries are able to get the direction sector information stored in the header of the message.

PROPOSED SYSTEM

To overcome this drawback new scheme is implemented and named as CASER. Here the data that is used for the secure transmission is energy balancing. Thus development of the proposed scheme is used for the energy balancing and for secure transmission. A secure and efficient Cost Aware Secure Routing (CASER) protocol is used to 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 trade-off 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.

System Overview

1. The Energy Balance Control (EBC) is the one of the problem in wireless sensor network. Here we discuss about the EBC. 1. Energy Balance Control (EBC): To balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels. The source node sends the message to neighboring nodes, then move to the next neighboring node.

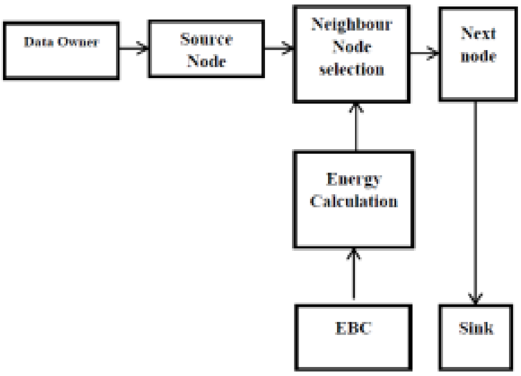

Fig.1.System Overview

The Fig 1 shows that, the data is sent the source node to destination node based on the neighbor's node selection. The EBC is the Energy Balance control; it is used to calculate the energy. The energy is calculating based on the EBC algorithm. First select the neighboring node for message forwarding. If the node is has the highest node means select that node. The sink node has the information about the entire node, that information is stored to the sink node. The source node sends the message to neighboring nodes, then move to the next neighboring node. Finally the message is send to sink node. In wireless sensor network, sink node has the all node information. The EBC method is used to calculate the energy for the sensor node.

MODULES DESCRIPTION

There are three modules:

1. Shortest path Allocation
2. Energy Balance Routing
3. Secure Routing Using CASER

A. Grid Creation

The network is normally deployed with number of sensor nodes .The network is divided into two or more equal size sections. The number of the sensor node is determined by the size of the grid. The number of sensor nodes in each grid follows id. When the number of sensor nodes in each grid is large. The sum of the energy in each grid should follow the normal distribution according to the central limit theorem. In our proposed dynamic routing algorithm, the next forwarding node is selected based on the routing protocol. The message is forwarding node based on the neighboring node selection and estimate the distance.

B. Energy Balance Routing

In the selection of the neighboring 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 α, αε [0, 1] 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 α, εα (A). The CASER path selection algorithm is derivate by the equation,

$$\varepsilon_\alpha(A) = \frac{1}{|NA|} \sum_{i \in NA} \varepsilon ri$$

Here ε is a parameter used for the Energy Balanced Control. And then the term α is used to denote challenging ratio. If α value is maximum means there is no shortest path in that node.

C. Secure Routing Using CASER

In the proposed model the data that are transmitted according to the routing strategy. A routing strategy that can provide routing path unpredictability and security the routing path become more changeable 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 N α A 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 N α A for message forwarding. The distribution of these two algorithms is controlled by a security level called βϵ [0, 1], carried in each message. When a node needs to forward a message, the node first selects a random number γϵ [0,1] If γ>β , 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. Smaller β results in a shorter routing path and is more energy efficient in message forwarding.

ALGORITHM

1. Energy Balance Control Algorithm

The energy Balance Control algorithm shows, 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 α A shrinks as a increases. In other words, as a increases, the routing flexibility may reduce. As a result, the overall routing hops may increase. But since ε α(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 α A.

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 1,500×1,500 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. We performed simulations with different α and β values. In all cases, we derived consistent results showing that the average number of routing hops derived in this paper provides a very close approximation to the actual number of routing hops. As expected, when the energy level goes down, the routing path spreads further wider for better energy balance. We also provided simulation results on end-to-end transmission delay in Table 1.

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 α can be adjusted to achieve the expected efficiency. As α increase, better energy balance can be achieved. Meanwhile, the average number of routing hops may also increase. Accordingly, the overall energy consumption may go up. In other words, though the energy control can balance the network energy levels, it may increase the number of routing hops and the overall energy consumption slightly. This is especially true when the sensor nodes have very unbalanced energy levels. In our simulations, shown in Fig. 2, the message source is located at (332, 259) and the message destination is located at (1,250, 1,250). The source node and the destination node are 10 hops away in direct distance. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. We show the remaining energy levels of the sensor nodes under two different α level.

TABLE 1 Delay Results for Various Security Parameters from Simulation

Security parmeter	**0**	**0.125**	**0.25**	**0.375**	**0.5**
Average delay(sec)	**0.0148**	**0.0177**	**0.0214**	**0.0265**	**0.0344**

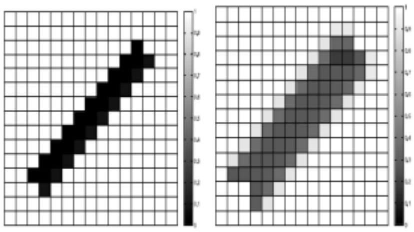
(a) α = 0 (b) α = 0.5

Fig.2. Remaining energy distribution statistics after the source transmitted about 600 messages.

The darker gray-scale level corresponds to a lower remaining level. Fig. 2a, we set α=0 and there is only one source node. The energy consumption is concentrated around the shortest routing path and moves away only until energy runs out in that area. In Fig. 2b, we set α = 0.5, then the energy consumption is spread over a large area between this node and the sink. While maximizing the availability of the sensor nodes, or lifetime, this design can also guarantee a high message delivery ratio until the energy runs out for all of the available sensor nodes in the area. We also conducted simulations to evaluate the energy consumption for dynamic sources in Fig.3. We assume that the only sink node is located in the center of the sensor domain. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. In this case, the energy consumption is highest for the node around the sink node. The consumption decreases based on the distance that the node is away from the sink node. In fact, the average energy consumption for the node with distance i to the sink node can be calculated as follows.

Theorem 5: Assume that all sensor nodes transmit messages to the sink node at the same frequency, the initial energy level of each grid is equal, then the average energy consumption for the grid with distance i to the sink node is

$$\frac{n^2+n+i-i^2}{2i}$$

Where n is the distance between the sink node and the outmost grid.

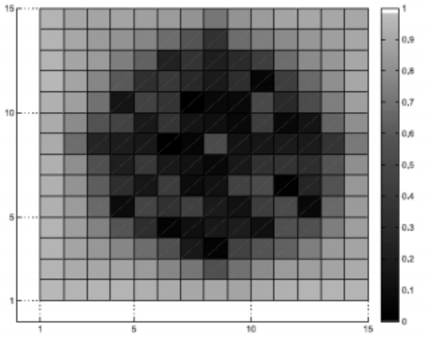

Fig.3. the remaining energy levels of the sensor nodes in the sensor domain when the innermost grid almost runs out of the energy, where α = 0.5, β = 0.5.

Proof: Since all messages will be sent to the sink node, the energy consumption for the grids with distance i to the sink node can be measured based on message forwarding for grids with distance larger than i and message transmission for grids with distance i. The number of grids with distance j to the sink node is 8j. The total energy consumption of the grids with distance i to the sink can be calculated as 8 : =1 the average grid energy consumption is therefore:

$$\frac{\sum_{j=1}^{n} 8j}{8i} = \frac{n^2 + n + i - i^2}{2i}$$

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 Figs. 3 and 4. 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. 3 gives the remaining energy levels close to the sink node when the sensor nodes run out almost the entire energy, where n = 7, α = 0.5, α = 0.5. The color evenness in each layer of the grids demonstrates the energy usage balance enforced through the EBC α. In fact, according to Equation (1), we can calculate the total number of messages that can be transmitted from the outmost grid when the innermost grid runs out of energy as210/((n 2 + n)/2)= 210/((72 + 7)/2= 7.5. In this case, the overall energy consumption is only 7.5× 8 =1 j 2 = 8,400, when the sensor networks become unavailable. Recall that the overall energy units deployed are 210× ((2n + 1)2 -1) = 47,040: Therefore, the energy consumption is only 8,400/47,040 = 5/28≈ 17.86% when the innermost grids run out of energy and become unavailable.

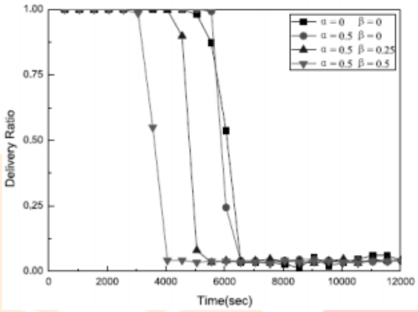

Fig.4. Delivery ratio under different EBC α and security level β

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 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. This has been confirmed through our simulations, shown in Fig.4.

CONCLUSION

To balance energy consumption and lengthen network lifetime, we introduced the Cost Aware Secure Routing (CASER) protocol for WSNs in this research. To increase routing security and lengthen the lifespan of messages, the CASER protocol supports several routing schemes. In terms of energy balance and routing path security, theoretical analysis and simulation results show that CASER has outstanding routing performance. The CASER protocol offers a non-uniform energy deployment strategy to extend the lifetime of the sensor network.

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 Networks”, IEEE Transactions on Parallel and Distributed Systems, 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. MiniConf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.
4. 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.
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, “Geographyinformed energy conservation for ad-hoc routing,” in Proc.7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

IJCRT

7. Y. Yu, R. Govindan, and D. Estrin,“Geographical and energy aware 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 fine grained localization in ad-hoc networks of sensors,” in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 200-1, 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. 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.
12. 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.

IJCRT