ENERGY-EFFICIENT RELIABLE ROUTING USING CASER PROTOCOL DESIGN FOR WSN

K.Anitta (PG Scholar), Prof.P.Arulprakash, M.E. (PH.D)
RVS College of Engineering and Technology, Coimbatore, TamilNadu.

Abstract: **A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. Routing is another very challenging design issue for WSNs. 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. It 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. It 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, It propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. For the non-uniform energy deployment, our analysis shows that It can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption.**

Keywords- **Message Delivery, CASER, Energy balance control, Random walking, Energy deployment, Energy consumption.**

1 INTRODUCTION

The recent technological advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both military and civilian applications, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. A key feature of such networks is that each network consists of a large number of untethered and unattended sensor nodes. These nodes often have very limited and non-replenishable energy resources, which makes energy an important design issue for these networks. 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. 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 trace back attacks and malicious traffic jamming attacks in WSNs.

1.1CHARACTERISTICS OF CASER

• 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.

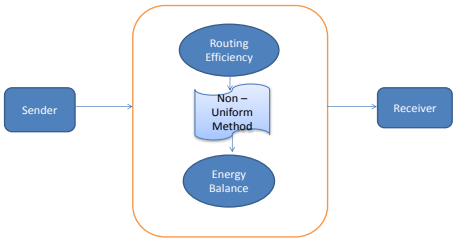

Fig.3.4 CASER Protocol (to using Energy-Efficient Reliable Routing method)

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. An efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. It also provides a quantitative security analysis on the proposed routing protocol. It can provide an excellent trade-off between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, to increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. To achieve a high message delivery ratio while preventing routing trace back attacks.

2. METHODS

2.1 EXISTING SYSTEM

A Wireless Sensor network consists of a large number of untethered and unattended sensor nodes. These nodes often have very limited and non-replenishable energy resources, which makes energy an important design issue for these networks. Routing is another very challenging design issue for WSNs. 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. In addition to the aforementioned issues, WSNs rely on wireless communications, which is by nature a broadcast medium. It is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In particular, in the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications. The adversaries may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not restricted to using sensor network hardware.
It is possible for the adversaries to perform jamming and routing trace back attacks. While geographic routing algorithms have the advantages that each node only needs to maintain its neighbouring 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. 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.

2.1.1. DRAWBACKS

The main drawbacks of existing system are:

- It cannot ensure balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.
- The secure message delivery does not to prevent routing trace back attacks and malicious traffic jamming attacks in WSNs.
- 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.

2.2 PROPOSED SYSTEM

Motivated by the fact that WSNs routing is often geography based, It propose a geography-based secure and efficient Cost- Aware Secure routing (CASER) protocol for WSNs without relying on flooding. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. In addition, it also gives quantitative secure analysis on the proposed routing protocol. 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. It devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment. It develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements. To propose an Energy Efficient Reliable Algorithm For our system then increasing a life time, energy efficiency, reliability in Energy-Efficient Reliable Routing. It 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. It 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, it proposes an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. It also provides a quantitative security analysis on the proposed routing protocol. Cost-Aware SEcure Routing (CASER) protocol 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 trade-off between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries.

2.2.1 ADVANTAGES

The advantage of the proposed system is as follows.

- It can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption.
- It can achieve a high message delivery ratio while preventing routing trace back attacks.
- 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 traceback attacks and malicious traffic jamming attacks in WSNs.
- While maximizing message source location privacy and minimizing traffic jamming for communication between the source and the destination nodes, it can optimize the sensor network lifetime through a balanced energy consumption throughout the sensor network.
- The energy levels of its adjacent neighboring grids, it can be used to detect and filter out the compromised nodes for active routing selection.

3. MODULES

3.1 ROUTE DISCOVERY

Initially all nodes collecting the data about neighbor nodes. The network monitors having the detailed information of neighbor nodes such as Routing table. It provides the connection information to Route manager.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 . 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. It proposes 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. For routing efficiency, It conduct simulations of the proposed CASER protocol using OPNET to measure the average number of routing hops for four different security levels. It randomly deployed 1000 sensor nodes in the entire sensor domain. It 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.

3.2 FAILURE DETECTION

The network monitors only provide the information about node details. Channel analyzer collecting detail about channel capability. If there is any problem with link channel then node will generate error message for inform about failure. 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 main idea is that the jammers try to interfere with normal communications between the legitimate communication parties in the link layer and/or physical layer. However, a jammer can perform attacks only when the jammer is on the message forwarding path. Dynamic routing is an effective method to minimize the probability of jamming. The CASER routing algorithm distributes 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.

3.3 ENERGY DEPLOYMENT STRATEGY

This module is energy deployment strategy to improve the network lifetime. It checks the resource availability, message delivery and security. It is non uniform method. The proposed CASER protocol using OPNET to measure the average number of routing hops for four different security levels. It randomly deployed 1000 sensor nodes in the entire sensor domain. It also assumes 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. It performed simulations with different ↵ and $ values. In all cases, It derived consistent results showing that the average number of routing hops derived It 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. 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 ↵, 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. 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. Under the new energy deployment, we have to redefine the way we calculate the average remaining energy of the adjacent neighboring grids since otherwise, the messages will always be routed to the nodes that are closer to the sink node, at least initially. In this way, the number of possible nodes for the next hop can be greatly limited and security routing may become trivial.

4. RESULTS & DISCUSSION

The energy consumption of the WSN for non-uniform energy deployment. Comparing the two results, It conclude that CASER can achieve excellent energy balance. All sensor nodes run out of energy at about the same time, while in uniform energy deployment, the energy consumption is very unbalanced. An excellent routing performance in terms of energy balance and routing path distribution for routing path security. It also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. Our analysis and simulation results of the output it can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four times. Recall that the 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. One of the major differences between our proposed CASER routing protocol and the existing routing schemes is that It 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. It implements 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.

5. CONCLUSIONS

CASER is designed to balance the energy consumption of sensor nodes and thereby extends the lifetime of the sensor networks. CASER protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking. 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. It allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. 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. We devised a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment. We developed theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements. 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.

5.1 FUTURE ENHANCEMENT

As future work, by reducing the bandwidth the energy consumption becomes less and the memory storage and the cost also becomes reduced. It is effective and flexible. The routing security gets increased. When comparing with the CASER protocol the above mentioned are more effective and also detects and removes the attacks in future.

REFERENCES

[1].J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, “A scalable location service for geographic ad hoc routing,” in MobiCom’2000. ACM, 2000, pp. 120 – 130.

[2].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.

[3].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].W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," IEEE Network, 2006.

[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.

[6]Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," 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," for mobile computing and communications, 1999, pp. 48–55.

[10]Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," VOL.2. 2006.

[11] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient in sensor networks," in Proc. IEEE INFOCOM, vol. 3, March 2004, pp. 1705 –1716 vol.3.

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

[13] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," WCNC2002. 2002 IEEE, vol. 1, 17-21 March 2002, pp. 350 – 355 vol.1.

[14] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," Networking, IEEE/ACM Transactions on, vol. 12, no. 4, pp. 609–619, August 2004.

[15] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks,"IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

