International Journal of Scientific Engineering and Innovative Research
Issue : 1 Volume : 1 Year : 2018

A Survey on Energy Charging & Deployment Technique against the Routing Strategy to optimize the lifetime and message delivery ratio of the WSN

Miss. NithyaKalyani
PG Scholar
RVS college of Engineering and Technology
Coimbatore , Tamilnadu

Prof. P.ArulPrakash,M.E(PhD)
RVS college of Engineering and Technology
Coimbatore , Tamilnadu

Abstract

Multi-Hop Wireless sensor networks (WSNs) use small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. As sensor networks become wide-spread, security issues become a central concern, especially in mission-critical tasks. Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenish able energy resources. In this paper, we first analyse a novel secure and efficient routing protocol to address these two conflicting issues through two adjustable parameters: energy balance control 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. 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.

Keywords: Routing, security, energy efficiency, energy balance, delivery ratio, deployment, simulation.

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 unmetered and unattended sensor nodes. These nodes often have very limited and non-replenish able 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. 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 traceback attacks. Motivated by the fact that WSNs routing is often geography based, we survey 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 [1]. 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. Our contributions of this paper can be summarized as follows: We Survey 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. 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. Theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements. We quantitatively analyze security of the proposed routing Algorithm. We provide an optimal non-

uniform energy deployment strategy for the given sensor networks based on the energy consumption ratio.

2. 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 [2]. The source chooses the immediate neighbouring node to forward the message based on either the direction or the distance [3]–[6]. The distance between the neighbouring nodes can be estimated or acquired by signal strengths or using GPS equipment [7], [8]. The relative location information of neighbour nodes can be exchanged between neighbouring nodes. In [5], 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 proposed in [6].

In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighbouring nodes based on estimated cost 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 in WSN. 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. To solve the local minimum problem, some variations of these basic routing algorithms were proposed in [9], including GEDIR, MFR an d compass routing algorithm. The delivery ratio can be improved if each node is aware of its 2-hop neighbours. There are a few papers [3], [10]–[12] discussed combining greedy and face routing to solve the local minimum problem.

The basic idea another area that has been extensively studied in WSNs. In [13], a routing scheme was proposed to find the suboptimal 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 [14], the authors 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 neighbouring node selection to maximize the network lifetime. Then [15] 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 perform data aggregation.

A localized zone-based routing scheme was proposed to balance energy consumption among nodes within each corona. The System has been formulated with integrated design of route selection, traffic load allocation, and sleep scheduling to maximize the network lifetime .Based on the concept of opportunistic routing developed a routing metric to address both link reliability and node residual energy. The sensor node computes the optimal metric value in a localized area to achieve both reliability and lifetime maximization. In addition, exposure of routing information presents significant security threats to sensor networks. By acquisition of the location and routing information, the adversaries may be able to trace back to the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design. 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. 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. Then every forwarder on the random walk path forwards this message to a random neighbour based on the direction/sector determined by the source node. 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 is able to get the direction/sector information stored in the header of the message.

Therefore, exposure of the direction decreases the complexity for adversaries to trace back to the actual message source in a two-phase routing algorithm to provide both content confidentiality and source-location privacy. The message is first transmitted to a randomly selected intermediate node in the sensor domain before the message is being forwarded to a network mixing ring where the messages from different directions are mixed. Then the message is forwarded from the ring to the sink node. In [1], 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 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. 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.

3. Overview

Attack models

The Attack model is classified into two major categories such as

- Passive attacks: Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis.
- Active attacks: Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in

the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

3.1. Message authentication: The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.

3.1.1. Node Characteristics for controlling attack

- Attack Characteristics of Node Controlling is employed through following scopes
- By capturing the single sensor node and make it to function abnormally.

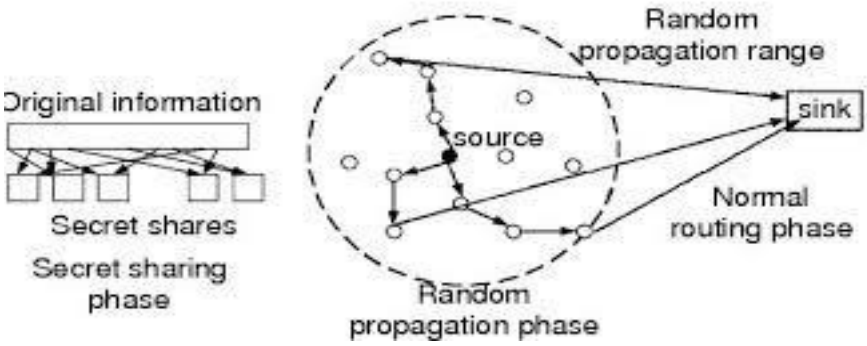
3.1.2. Packet Modification Attack Characteristics

- It is caused due the packet is compromised and accessed by the attacker
- Packet header information is revealed to the attacker to launch other serious of attacks

3.2. Overview of the Secured Scheme

Symmetric Key Cryptosystem

Symmetric authentication key is shared by a group of sensor nodes.



Therefore, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. In Fig.1, we explain the node aggregation of Wireless sensor Network schemes, including TESLA and its variants, can also provide message sender authentication. This scheme requires initial time synchronization, which is not easy to be

implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up.

3.3. ECC algorithm for Message Security based on ELGamal scheme

An alternative solution was proposed to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add a random noise, also called a perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved. However, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. One of the limitations of the public-key based scheme is the high computational overhead.

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve- based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.

3.4. Source Privacy the Source anonymous message authentication algorithms

The appropriate selection of an AS plays a key role in message source privacy, since the actual message source node will be hidden in the AS. In this section, we will discuss techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis. Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes. When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real node of the previous hop. However, the adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node if the adversary is unable to monitor the traffic of the previous hop. Some basic criteria for the selection of the AS can be described as follows:

To provide message source privacy, the message source needs to select the AS to include nodes from all directions of the source node. In particular, the AS should include nodes from the opposite direction of the successor node. In this way, even the immediate successor node will not be able to distinguish the message source node from the forwarder based on the message that it receives. The information maintained by each sensor node will be updated periodically We assume that the sensor nodes in its direct neighbouring grids are all within its direct communication range. We also assume that the whole network is fully connected through multi-hop communications. While maximizing message source location privacy and minimizing traffic jamming for communications between the source and the destination nodes, we can optimize the sensor network lifetime through a balanced energy consumption

3.5. Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks

Unbalanced energy consumption is an inherent problem in wireless sensor networks characterized by multihop routing and many-to-one traffic pattern, and this uneven energy dissipation can significantly reduce network lifetime. In this paper, we study the problem of maximizing network lifetime through balancing energy consumption for uniformly deployed data-gathering sensor networks. We formulate the energy consumption balancing problem as an

optimal transmitting data distribution problem by combining the ideas of corona-based network division and mixed-routing strategy together with data aggregation. We first propose a localized zone-based routing scheme that guarantees balanced energy consumption among nodes within each corona. We then design an offline centralized algorithm with time complexity O(n) (n is the number of coronas) to solve the transmitting data distribution problem aimed at balancing energy consumption among nodes in different coronas. The approach for computing the optimal number of coronas in terms of maximizing network lifetime is also presented.

4. Conclusion

In this survey , we discussed 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 analysed 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.

5. Reference

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

[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.

[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. Workshop on Discrete Algorithms and methods for mobile computing and communications, 1999, pp. 48–55.

[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.

[11] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing 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 greedy, face, and 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," in Wireless Communications and Networking Conference, 2002. 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," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.