www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 15045-15048

Providing Lifetime Optimization and Security in Wireless Sensor Network

Sindhuja.R, Mrs.Vidhya.S
PG Student& Assistant Professor
Computer Science and Engineering & Anna University
Ponjesly College of Engineering, Tamil Nadu, India,
rsindhu17@gmail.com
vidhya.mahesh@ymail.com

Abstract - Wireless sensor network is a self-organized wireless network system constituted by numbers of energy-limited micro sensors under the banner of industrial application (IA). In this project, a secure and efficient cost aware securer routing protocol to address two conflicting issues: they are lifetime optimization and security. Through the energy balance control and random walking the conflicting issues are addressed. Then discover 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 an efficient non-uniform energy deployment strategy is used to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. It is also to provide a quantitative security analysis on the proposed routing protocol.

Keywords: wireless sensor network, cost aware, secure routing protocol, lifetime optimization, energy consumption, uniform energy, deployment, strategy, security.

I. INTRODUCTION

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 unattended sensor nodes. The 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 wireless sensor network energy consumption, and there by extend the sensor network lifetime. Motivated by the fact that WSNs routing is often geography-based 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 wireless 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.

Our contributions of this paper can be summarized as follows:

- 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.
- The 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 (ED).
- Theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.
- Analyse security of the proposed routing algorithm. It provides an optimal non-uniform energy deployment (non ED) strategy for the given sensor networks based on the energy consumption ratio.
- The theoretical and simulation results both show that under the same total energy deployment. It can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

II. 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.

III. 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 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. 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.

IV. SYSTEM OVERVIEW

The Energy Balance Control (EBC) is the one of the problem in wireless sensor network. Here we discuss about the EBC.

A. 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 send the message to neighbouring nodes, then move to the next neighbouring node.

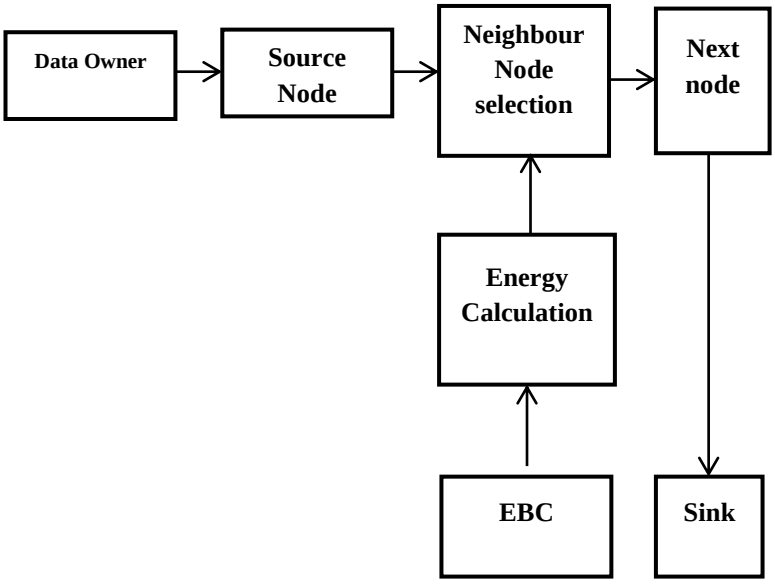


Fig 1.System Overview

The Fig 1 shows that, the data is sent the source node to destination node based on the neighbour'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 neighbouring 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 neighbouring nodes, then move to the next neighbouring 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.

V. 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 neighbouring node selection and estimate the distance.

B. Energy Balance Routing

In the selection of the neighbouring 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, $\alpha\epsilon[0,1]$ 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 $\alpha\ \epsilon_\alpha$(A).

The CASER path selection algorithm is derivate by the equation,

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

Here ε is a parameter used for the Energy Balanced Control. And then the term $\alpha\ is$ used to denote challenging ratio. If the 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_A^α based on the relative locations of the grids.

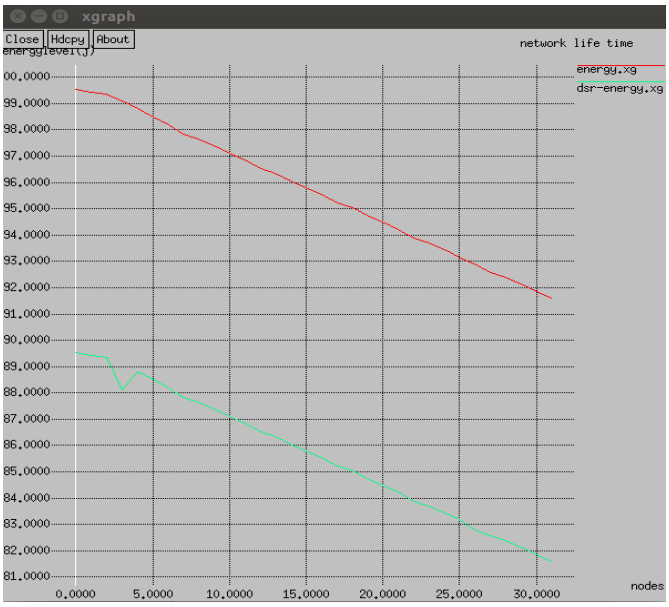
The grid that is closest to the sink node is selected for message forwarding. In the secure routing case, the next hop grid is randomly selected from N_A^α for message forwarding. The distribution of these two algorithms is controlled by a security level called βϵ[0,1], carried in each message.

When a node needs to forward a message, the node first selects a random number $\gamma\epsilon[0,1]$ If γ>β, then the nodeselects the next hop grid based on the shortest routing algorithm; otherwise, the next hop grid is selected using random walking. The security levelβ, is an adjustable parameter. A smaller β results in a shorter routing path and is moreenergy efficient in message forwarding.

VI. ALGORITHM

A. 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_A^α 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 N_A, this subset is dynamic and will never be empty. Therefore, the next hop grid can always be selected from N_A^α .



PERFORMANCE ANALYSIS

The CASER protocol provides the network lifetime and increasing the security for wireless sensor networks.

Fig 2.Network Lifetime

The Fig 2 shows that, a x graph is plotted for network life time. X-axis denotes the number of nodes and Y-axis denotes the energy level(J). The energy level unit is joule. Compare to the existing system proposed system network lifetime is increasing. Red colour line denotes the increasing energy and green colour line denotes the delivery ratio for energy.

VII. RELATED WORK

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 in WSNs. In CASER protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighbouring grids and 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. Our extensive simulation results show that CASER can provide excellent energy balance and routing security.

VIII. 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 protocol is support multiple routing strategies in message forwarding to extend the lifetime and increasing routing security. Both theoretical analysis and simulation results provide that CASER has an excellent routing performance in terms of energy balance and routing path security. The CASER protocol provide a non-uniform

energy deployment scheme to maximize the sensor network lifetime.

begin
initialize A node
set of its adjacent neighboring grids as NA
the remaining energy of grid i as εri
a parameter $\alpha \in [0,1]$
else
α increases from 0 to 1
end

REFERENCES

[1] Di Tang, Tongtong Li, Jian Ren, "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. Mini-Conf., 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, "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.
[7] 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.
[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. 00729, Apr. 2000.
[9] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.