ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

AN ENERGY BALANCE CONTROL AND SECURE ROUTING PROTOCOL DESIGN FOR WIRELESS SENSOR NETWORK

S.Mohamed Nisha[1], S. Ramesh [2]
[1]Pg Scholar, Anna University Regional Campus, Madurai, India
[2]Professor/CSE, Anna University Regional Campus, Madurai, India
snishanazar@gmail.com, rameshcse@autmdu.ac.in

Abstract- A wireless sensor network is a set of specialized transducers with a communications infrastructure deployed in an ad hoc fashion. The potential application of WSN are monitoring of weather conditions, robot control, marine life monitoring, military surveillance etc. In all these applications major conflicting issues are lifetime optimization of sensor nodes and secure transmission of messages is needed for an efficient network processing. In this paper we propose a secure and efficient Cost –Aware Secure Routing protocol to balance the energy consumption and security level using two adjustable parameters: EBC and probabilistic based random walking .In a network topology the consumption of energy is intensely disproportional to the uniform energy deployment, to a great extent it reduces the sensor network lifetime. This issue can be solve by placing sensors in different densities termed as non- uniform energy deployment results in balanced consumption of energy under the same requirements and resources. Simulation results shows that in all the scenarios CASER protocol can provide better proportion between routing and energy balance .Analysis results also show that the life time of sensor networks can be improved and it also anticipate routing trackback attacks.

Keywords—CASER protocol , Network Lifetime, Routing protocol , Energy balance control , Jamming attack .

I. INTRODUCTION

WIRELESS sensor networks (WSNs) have been intended as a technology that has an abundant capacity to be widely used in both civilian and military applications where Sensor networks depend on wireless communication, by nature it's a broadcast medium and is more exposed to security attacks than its wired broadcast due to absence of a physical boundary. Sensor networks usually contains hundreds of nodes where each node is connected positioned for the persistence of environment examining and control. The required information can be retrieved by inserting queries from the network.Though networking and security machineries are in a progressive stage, wireless sensor networks present convolutions which dictate the scheme of new protocols.

First, these grids organize in an infrastructure-less ad hoc manner, which denotes that the interaction relies on the collaboration between nodes for the attainment of basic networking tasks such as routing. Each time a sensor requests to send the recognized value to the data basin, it glances for an available neighbor. As these are ad hoc networks planned to organize in a self-organized fashion, a malicious node may arrive the network. Due to the wireless strategy, snooping can be easily achieved in this environment which creates the network vulnerable not only to privacy attacks, but also to traffic exploration attacks which threaten the whole grid operation.

Cryptography and authentication can assist but do not avail due to the constraints described. To this end, security is extremely vulnerable in wireless sensor networks and the routing system is at the focus of adversaries due to its significance for the suitable network operation and its vulnerability led by the required collaboration. The up to date interest in sensor networks has headed to a number of routing patterns that use the limited resources available at sensor nodes more efficiently.

Routing is the essential design concern for WSN. A well planned routing protocol provides a smaller amount of energy depletion for communication and has the good message delivery ratio. To expand the Sensor network lifetime and also manage entire sensor network energy depletion.

Wireless Sensor Networks have the solution which supports extensive range of applications. Based on the type of application, their WSN environs it is the risky, perplexing and rarer problematic. Even the programmed Security schemes in WSNs not to observe the node tangible internment, the malicious nodes. So unique security systems is important for the secure transmission of message from source to sink. A novel system of attaining security in absence of cryptography is defined as Trust based security where Trust is termed as -The sign of Trustworthiness. It collects the nodes information and observes the action of other nodes as well as the details of communication in the grid either directly or indirectly. By using all these information trust value will be calculated. To look after the decision making methods of the network Trust management will be used and it also helps to identify the unsecured nodes.

Several observations on trust related with WSN are done, but it is critical to design and develop a trust management scheme which uses the minimum amount of resources of the node and also to maintain the trust among the nodes in the grid. In a Wireless Sensor Network trust management will be as a simple one if it doesn't have the limitations on consumptions of energy, and easy to adopt the changes.

The rest of this project is organized as follows: Chapter 2 explains the related work of the project. Chapter 3 discusses the system architecture. Chapter 4 explains the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

design principles of Two tier energy efficient secure key management. Chapter 5 provides the simulation results of the Two tier energy efficient secure key management. Chapter 6 concludes the project with future work.

II. RELATED WORK

In wireless sensor networks conventional routing protocols cannot be used directly due to the constraints enacted in sensor nodes like handling abilities, transmission and power usage. Hence in order to solve routing problem in wireless sensor networks Lots of algorithm have been anticipated among those Geographic routing was mostly perceived as an essential approach . In Geographic routing it make use of the location information to transmit data packets from source to destination in hop-by-hop manner[2]. Based on the available information or distance calculated the source decides the next node to pass the information. The distance stuck between the adjacent nodes can be estimated by signal strengths or using GPS [7], [8]. The relative position info of neighbor nodes can be exchanged between other nodes in the grid.

Gradient based routing was first proposed by Schurgers et al. in GBR [3]. Their proposed protocol is a modified version of Directed Diffusion [2].The main concept of their anticipated protocol is to have minimum number of hops towards the sink. GRACE [7] forms a usual gradient near the sink where gradient is the term defines link cost between a node and its neighbors. From that, minimum cost to reach the sink will be calculated. The gradient based routing is based on the fact that route for the transmission in grid is always known, that is, from the source to the sink.

GEAR (geographic and energy aware routing) A query based technique was proposed in [6]. In GEAR, the sink node propagates requests with physical attributes to the target zone as a replacement for flooding. Each node in the grid communicates with its neighboring nodes based on estimated cost and learning cost. The estimated cost involves both the remaining energy of the sensor nodes as well as the distance to the destination .Where the learning cost specifies the updating information to deal with the local minimum problem.

While geographic routing algorithms have the pros that each node only desires to preserve its neighboring node information, and deliver a higher efficiency and a better scalability in case of large scale WSNs, these algorithms may reach their local minimum, which can result in dead end or hoops. To elucidate the local minimum problem, some disparities of these basic routing algorithms were proposed in [9]

In Wireless sensor networks another major issue is Lifetime of sensor nodes and it also plays a key role. In [13], a routing system was defined to analyze the sub-optimal path that can lengthen the lifetime of sensor nodes instead of choosing the lowermost energy path. AODV is also a responsive protocol to route multiple paths and to provide a secure routing strategy. The route can be chosen based on a probabilistic approach with respect to the remaining energy level of the sensor node. Based on the distance between the transmitter and the receiver power level can be adjusted. The sensor node computes the finest value in a localized area to accomplish both reliability and lifetime enlargement.

III. GOALS OF CASER PROTOCOL

CASER(Cost-Aware SEcure Routing)protocol that can address both energy balance and routing security simultaneously in Wireless Sensor Networks. In CASER protocol, each and every sensor node in the grid must have to maintain the energy levels of its immediate adjacent neighboring nodes including their relative locations. With this information, each sensor node can generate varying filters based on the estimated design tradeoff involving both security and efficiency.

The goal of this protocol is to maximize the sensor network lifetime by balancing the energy consumption among the nodes in the grid, to improve the message delivery ratio by reducing message drop and to protect the source location information from the adversaries.

IV. PROPOSED SYSTEM

We describe the proposed CASER protocol. In this scheme, routing assessments can vary to put emphasis on multiple routing schemes. In this paper, we will concentrate on two different routing strategies for transmission of message they are shortest path message forwarding, and secure message forwarding over and done with random walking to generate routing path unpredictability for secure transmission and to reduce congestion. As termed earlier, we are fascinated in routing schemes that can balance consumption of energy.

A. Network establishment

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

The system is designed for safe and secure routing of Information among the nodes. The networks are self-possessed with huge number of sensors and sink node. Each and every node in the grid has an inadequate and non-replaceable energy resource. The sink node is considered as a target for all sensor nodes to transmit data through multi-hop routing scheme. The network is uniformly divided into small grids. Each grid in the network carries relative location based on the data. The node which retains maximum level of energy is designated as the dome node for message forwarding. All the nodes in grid will uphold its own features, including location info, residual energy level and also the attributes of its adjacent node. The information preserved by each sensor node will be updated from time to time.

B. Energy Balance and Secure Routing Strategy

The CASER protocol is aimed to balance the whole sensor network and its energy consumption in all the grids by monitoring energy outgoings from sensor nodes with low-slung energy levels. In this process, we can lengthen the lifetime of the sensor networks in the grid. Through the Energy Balance Control, energy intake from the sensor nodes with comparatively lower energy levels can be delimited and controlled. Therefore, we can efficiently avoid any major sections of the sensor area from entirely running out of energy and becoming unattainable.

we simulate that each node in the grid retains its virtual location and the residual energy levels of its adjacent neighboring node in grids. For node A, represent the set of its immediate adjacent nodes as N(a) and the remaining energy level *i* where E(*i*) belongs to N(a). With this data, the node A can work out the average residual energy of the grids in N(a) as E(a) .In the multi-hop routing protocol, node A chooses its succeeding hop grid only from the set N(a) according to the determined routing scheme. To accomplish energy balance between all the grids in the network, we cautiously monitor and manage the energy depletion among the nodes with relatively minimum energy levels by designing A to only select the grids with relatively remains with maximum level of energy for message forwarding.

Algorithm: To find the next hop grid by balancing the energy level

Step 1: Calculate the average remaining energy of the adjacent neighboring grids in the network

$$E(a) = 1/N(a) \sum i \in N(a)\mathrm{E(r)}$$

Step2: Decide the contender grids for the next routing hop

Step 3: Transmit the message to the grid in the N(a) that is next to the sink node based on its relative location.

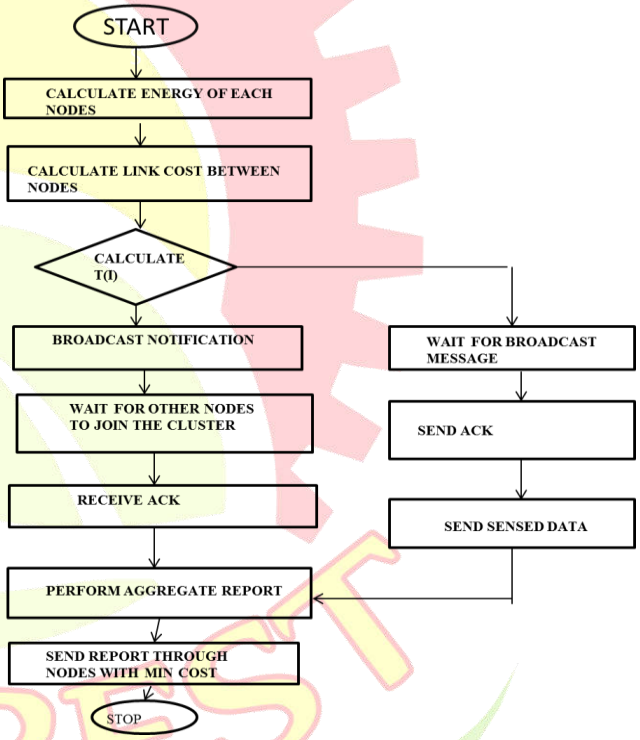

Fig 1: Defines the flow that takes place while executing the Caser protocol.

Energy Distribution Analysis:

Assume that each and every sensor node is initially organized with equal amount of an initial energy. The energy level drops when the sensor node transmits the data packets. The residual energy level of each node is rest on on the events distribution. Since the event is a random variable in the network and the remaining energy levels are considered as a random variable. In the meantime the network is randomly organized. The quantity of sensor nodes in each grid is calculated by the size of the grid.

Secure Routing Strategy

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

In the prior section, we only defined the shortest path routing selection approach. Though, in CASER protocol, we can upkeep other routing strategies. In this segment, we propose a routing strategy that can deliver routing path unpredictability and provides security. The routing protocol encloses two options for message forwarding: one is a deterministic shortest path routing and the other is a secure routing algorithm through random walking.

In the deterministic routing approach, the next hop grid is selected from N(a) based on the relative locations of the grids. The grid that is next to the sink node is carefully chosen for message forwarding. In the secure routing situation, the next hop grid is randomly selected from N(a) for data transmission . The dissemination of these two algorithms is monitored by a security level.

If a node desires to transmit a message, first the node pick out a random number then the node chooses shortest routing algorithm for the next hop; else, the next hop is a selection by using random walking. The security level is defined as an adjustable parameter. Larger the security level provides higher routing and security in case of shorter value it results in efficient energy.

Algorithm 2:

Step 1: calculate the average residual energy of the nearest nodes in the grid

$$E(a)=1/N(a)\sum_{i\in N(a)} E(r)$$

Step 2: Find the next node in the grid for further hoping

Step 3: Select a random number x∈(0,1)

Step 4:if x>y then

Forwards the data packet that is closest to the sink based on its relative location;

Step 5: else

Forwards the data packets to randomly selected grid;

End if

The routing path turns out to be more active and unpredictable. In this way, it is grimmer for the adversary to internment the data or to jam the traffic.

V. SIMULATION RESULTS

Simulations conducted using Ns2 to compare the message delivery ratio of uniform energy deployment (noED) and non-uniform energy deployment (ED) for different values. The simulation locations are akin. Though, each node is organized with a different energy level according to Algorithm.

A. Energy consumption

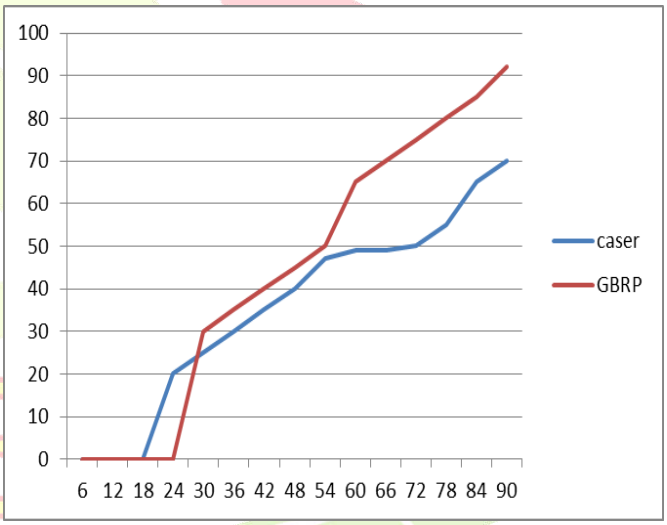

Fig 2: **X-axis** represents **time period** in seconds and **Y-axis** represents **data packets**. Higher the consumption of Energy reduces the lifetime of sensor networks hence by using CASER protocol it reduces the consumption of energy than the Existing.

B. Packet Delivery Ratio

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

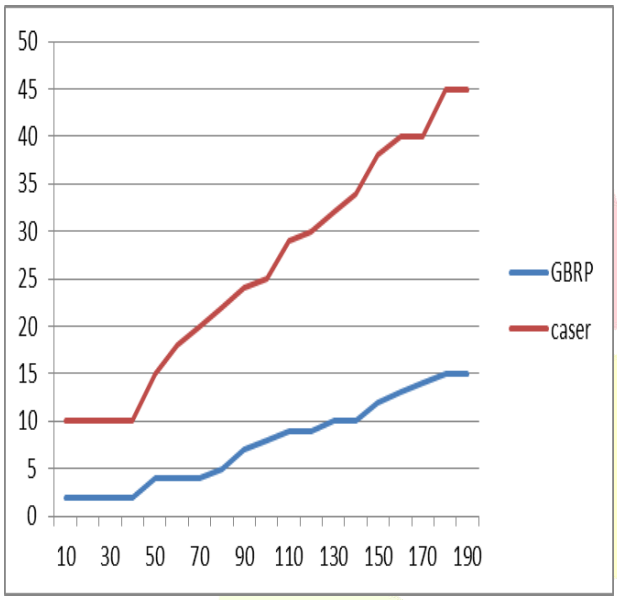

Fig 3: **X-axis** represents **time period** in seconds and **Y-axis** represents **data packets.** The ratio represents the amount data packets delivered from source to the destination. Data delivery ratio is improved when comparing to the existing GBRP.

C. Throughput

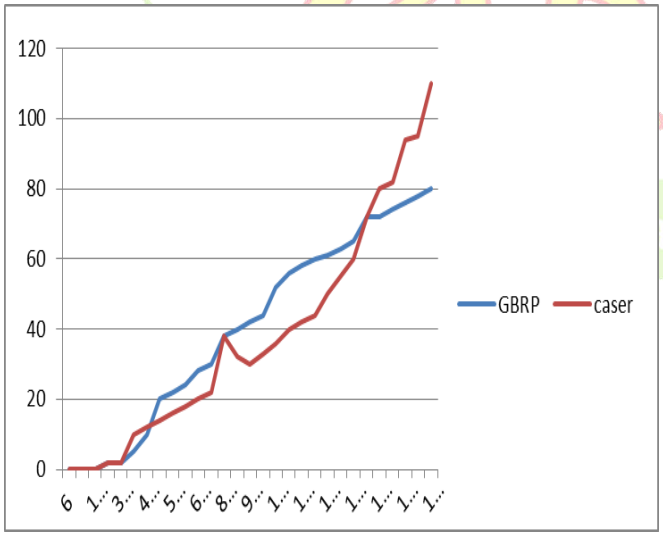

Fig 4: **X-axis** represents **time period** in seconds and **Y-axis** represents **data packets.** Throughput represents the amount of work done in a given time. Simulation results show that Throughput is increased when compared to the existing protocol.

VI. CONCLUSION

In this paper, we proposed a secure and efficient CASER(Cost-Aware SEcure Routing protocol) for Wireless Sensor Networks to maintain the consumption of energy and results in the increased network lifetime. CASER provides support to multiple routing strategies in forwarding message to maximize the lifetime with increased routing security. CASER result in an excellent routing presentation in terms of energy consumption and routing path distribution for security by calculating theoretical study as well as the simulation results. To maximize the lifetime of the sensor network we also anticipated a non-uniform energy deployment scheme. The results from Analysis and simulation indicate that we can extend the lifetime of sensor networks and the amount of data that can be transmitted under the non-uniform energy deployment by more than four times.

REFERENCES

1]Chang J.H and Tassiulas.L, "Maximum lifetime routing in wireless sensor networks,"Networking, IEEE/ACM Transactions on, vol. 12, no. 4,pp.609619,August 2004

[2]Di Tang, Tongtong Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow,IEEE Vol.26,No.4.April 2015 Cost-aware secure routing protocol for wireless sensor networks

[3]Hung.C.C, Lin.K.J, Hsu.C.C, Chou.C.F, and Tu.C.J, "On enhancing network-lifetime using opportunistic routing in Wirelesssensor networks," in Proc. 19th Int. Conf. Comput. Commun.Netw., Aug. 2010, pp. 16.

[4]Kamat.P, Zhang.Y, Trappe.W, and Ozturk.C, "Enhancing source location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib.Comput. Syst., Jun. 2005, pp. 599608

[5]Kamat.P, Zhang.Y, Trappe.W, and Ozturk.C, "Enhancing source location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib.Comput. Syst.,Jun. 2005, pp. 599608.

[6]Karp.B and Kung.H.T, "GPSR: Greedy perimeter stateless routing for wirelessnetworks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY,USA, 2000, pp. 243254.

[7]Li M., Li Z., and VasilakosA.V.(2013), 'A survey on topology control in wireless sensor networks: taxonomy, comparative study, and open issues,'Proceedings of the IEEE, Vol. 101, No. 12, pp. 25382557.

[8]Li.Y and Ren.J, "Preserving source location privacy in wireless sensornetworks," in Proc. IEEE 6th Annu. Commun. Soc. Conf.Sens., Mesh Ad Hoc

Commun. Netw., Rome, Italy, Jun. 2009, pp.493501.

[9]Liu .F, Tsui .C, and Zhang.Y .J(2010), "Joint routing and sleep scheduling For lifetime maximization of wireless sensor networks,"IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 22582267.

[10]Ozturk.C, Zhang.Y, and Trappe.W, "Source location privacy in energyconstrained sensor network routing," in Proc. 2nd ACM Workshop Security AdHoc Sens. Netw., 2004, pp. 8893.

[11]Pathan.A, Lee.H.W, and seon Hong.C, "Security in wireless sensor networks:Issues and challenges," in Proc. 8th Int. Conf.Adv. Commun.Technol., 2006, pp.10431048.

[12]Savvides,Han.C, and SrivastavaM.B.(2001), "Dynamic fine grained localization in adhoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf.Mobile Comput. Netw., pp. 166179.

[13]Shah.R and Rabaey .J(2002),"Energy aware routing for low energy adhoc sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., vol. 1, pp.350355.

[14]Xu.Y,Heidemann.J, and Estrin .D(2001), "Geography informed energy conservation for adhoc routing," in Proc. 7th Annu. ACM/IEEEInt. Conf. Mobile Comput. Netw, pp. 7084.

[15]Xu.w, Ma.k,Trappe.w, and Zhang.y, "Jamming sensor networks:attack anddefense strategies,"IEEE Network, vol. 20, no. 3, pp. 4147,2006.