ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Design of CASER Protocol for WSN

Dhanyashree P N[1], Prashanth C R[2]

PG (M Tech, DCN) Student, Dr. AIT, Bangalore, India[1]

Professor, Dr. AIT, Bangalore, India[2]

ABSTRACT: It is well known that wireless sensor networks (WSNs) is a self-organization wireless network system constituted by numbers of energy-limited micro sensors under the banner of industrial application (IA). In this project, we propose a secure and efficient Cost Aware Secure Routing
(CASER) protocol to address two conflicting issues; they are lifetime optimization and security. Through the energy balance control and random walking, we can address those conflicting issues. 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.

KEYWORDS: wireless sensor network, uniform energy deployment, non uniform energy deployment.

I. INTRODUCTION

A wireless Sensor Network (WSN) consists of hundreds or thousands of sensor nodes and a small number of data collection devices. The sensor nodes have the form of low cost, low-power, small-size devices, and are designed to carry out a range of sensing applications, including environmental monitoring, military surveillance, fire detection, animal tracking, and so on. The sensor nodes gather the information of interest locally and then forward the sensed information over a wireless medium to a remote data collection device (sink), where it is fused and analyzed in order to determine the global status of the sensed area.
The basic structure of Wireless Sensor Networks is shown in figure 1.1.

A key feature of such networks is that each network consists of a large number of un tethered 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.
The main feature of WSNs can be deduced as: scalability with respect to number of nodes, self organization, self healing, energy efficiency, lifetime optimization, low complexity, low cost, security, routing, and size of nodes and connectivity between the nodes. Every node in the network may either be a source or destination or not both also. CASER protocol has two major advantages:

1. It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.
2. 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.
   In this paper “design of CASER protocol for WSNs, life optimization, security and routing are taken as conflicting design issues for multihop WSNs. Initially a source and efficient protocol is proposed to acquire these issues.

   Two parameters are used:
   1. Energy balanced control (EBC).

2. Probabilistic random walking.

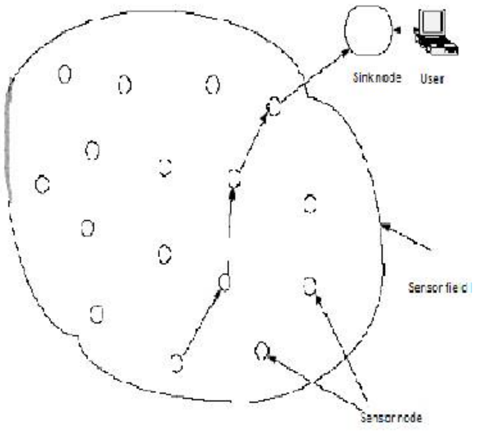


Fig: 1.1 basic structure of WSN

Our contributions of this paper can be summarized as follows:

1) 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.
2) We 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 (ED).
3) We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.
4) We quantitatively analyze security of the proposed routing algorithm.
5) We provide an optimal non-uniform energy deployment (noED) strategy for the given sensor networks based on the energy consumption ratio.

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.

The simulation and theoretical results show that lifetime is extended and also the number of messages delivered is more than four times in non-uniform energy deployment strategy.

II. 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].

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 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 and compass routing algorithm.

The delivery ratio can be improved if each node is aware of its two-hop neighbors. There are a few papers [3], [10], [11], [12] discussed combining greedy and face routing to solve the local minimum problem. The basic idea is to set the local topology of the network as a planar graph, and then the relay nodes try to forward messages along one or possibly a sequence of adjacent faces toward the destination.

Lifetime is another area that has been extensively studied in WSNs. In [13], a routing scheme was proposed to find the sub-optimal 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], Chang and Tassiulas 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 Zhang and Shen [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.

Subramanian and Katz [11] not only describe a self-organizing protocol but develop taxonomy of sensor applications as well. Based on such taxonomy, they have proposed architectural and infrastructural components necessary for building sensor applications. The architecture supports heterogeneous sensors that can be mobile or stationary. Some sensors, which can be either stationary or mobile, probe the environment and forward the data to designated set of nodes that act as routers. Router nodes are stationary and form the backbone for communication. Collected data are forwarded through the routers to more powerful sink nodes. Each sensing node should be reachable to a router node in order to be part of the network.

A routing architecture that requires addressing of each sensor node has been proposed. Sensing nodes are identifiable through the address of the router node it is connected to. The routing architecture is hierarchical where groups of nodes are formed and merge when needed. In order to support fault tolerance, local Markov loops (LML) algorithm, which performs a random walk on spanning trees of a graph, is used in broadcasting.

The algorithm for self-organizing the router nodes and creating the routing tables consists of four phases:
- Discovery phase: The nodes in the neighbourhood of each sensor are discovered.
- Organization phase: Groups are formed and merged by forming a hierarchy. Each node is allocated an address based on its position in the hierarchy. Routing tables of size Oðlog NÞ are created for each node. Broadcast trees that span all the nodes are constructed.
- Maintenance phase: Updating of routing tables and energy levels of nodes is made in this phase. Each node informs the neighbors about its routing table and energy level. LML are used to maintain broadcast trees.
- Self-reorganization phase: In case of partition or node failures, group reorganizations are performed.

In section 2, the related work of his paper is discussed. In section 3, the proposed methodology i.e., CASER protocol is described, the working, algorithm and the flow of data is determined. Section 4 describes the models and assumptions in which the system model, overview of the system, the modules description are explained. In section 4, we speak about the simulation, NS2 the basic architecture of NS2. And the experimental results are shown in the section 7.

III. PROPOSED METHOD

Proposed work is about balancing the energy efficiency and security of wireless sensor network. To make this possible we are using watchdog optimizing technique in two levels.

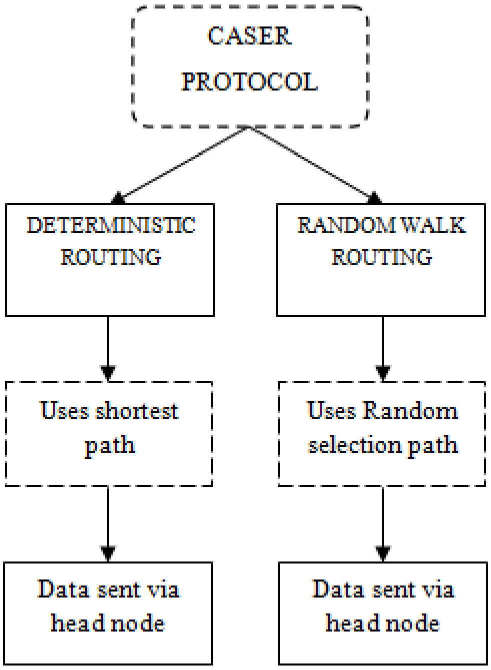


Fig: 3.1 Levels of CASER Protocol

That is random walking and deterministic routing. The security requirements determine the distribution of these two strategies. This protocol provides maximum delivery ratio by assuring secure message delivery under adversarial attacks.

By the survey CASER protocol has two advantages:

i. It provides balance energy consumption of the entire sensor network therefore the lifetime of network can be optimized.

ii. Multiple routing strategies are supported by CASER protocol. Multiple routing strategies is based on the routing requirements, such as fast/slow message delivery in order to avoid routing traceback attacks and traffic jamming attacks in WSNs.

We assume that the WSNs are composed of a large number of sensor nodes and a sink node. The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node has a very limited and non-replenishable energy resource. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy. The information of the sink node is made public. For security purposes, each message may also be assigned a node ID corresponding to the location where this message is initiated. To prevent adversaries from recovering the source location from the node ID, a dynamic ID can be used. The content of each message can also be encrypted using the secret key shared between the node/grid and the sink node.

We also assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels of the grid. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update.

Advantages

1. Reduce the energy consumption
2. Provide the more secure for packet and also routing
3. Increase the message delivery ratio

4. Reduce the time delay

The network is evenly divided into small grids.

Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node or message forwarding. In addition, each node in the grid will maintain its own attributes, including location information remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids. 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.

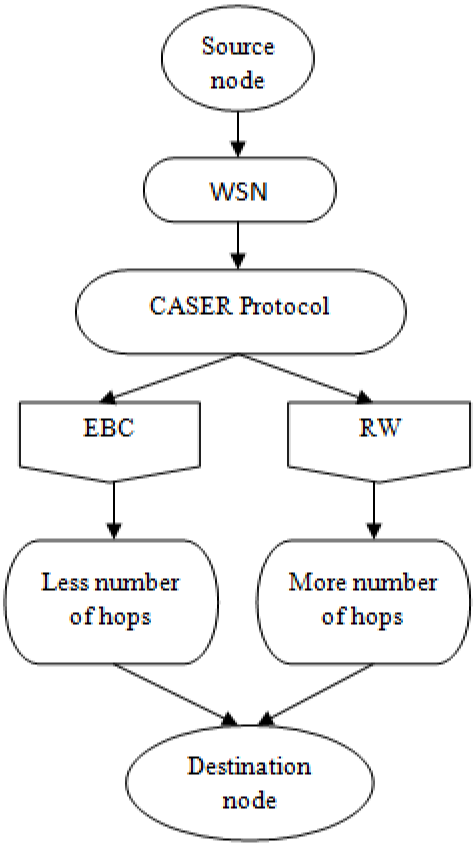


Fig2. Flow chart of data transaction in WSN

IV. MODELS AND ASSUMPTION

4.1. System model

We assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels of the grid. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update.

In this paper, we will not deal with key management, including key generation, key distribution and key updating.

4.2. The Adversarial Model and Assumptions

In WSNs, the adversary may try to recover the message source or jam the message from being delivered to the sink node. The adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes. In

this paper, the adversaries are assumed to have the following characteristics:

1) The adversaries will have sufficient energy resources, adequate computational capability and enough memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without too much delay. They may also compromise some sensor nodes in the network.
2) The adversaries will not interfere with the proper functioning of the network, such as modifying messages, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping on the communications.
3) The adversaries are able to monitor the traffic in any specific area that is important for them and get all of the transmitted messages in that area. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire WSN, they can monitor the events directly without relying on other people's sensor network.

4.3. Design Goals

Our design goal can be summarized as follows:

a. To maximize the sensor network lifetime, we ensure that the energy consumption of all sensor grids are balanced.
b. To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping when an alternative routing path exists.
c. The adversaries should not be able to get the source location information by analyzing the traffic pattern.
d. 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.
e. 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.
f. 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.

4.4. Overview of the Proposed Scheme

In our scheme, the network is equally partitioned into small grids. Every grid has a relative area taking into account the grid information. The node in every grid with the highest energy level is chosen as the head node for message transmission. Moreover, every node in the grid will keep up its own qualities, including location information, available energy level of its grid, and in addition the qualities of its adjoining neighbouring grids. The data kept up by every sensor node will be upgraded intermittently. We expect that the sensor nodes in its direct neighbouring grids are all inside its immediate communication range. We additionally accept that the entire network is completely associated through multi-hop communication.

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 balanced energy consumption throughout the sensor network.

Moreover, the kept up energy levels of its contiguous neighbouring grids can be utilized to distinguish and sift through the traded off nodes for dynamic routing determination.

The main conflicting issue is Energy Balance Control (EBC) in wireless sensor network.

Energy Balance Control (EBC):

To balance the general sensor system energy consumption in all grids by controlling energy going through from sensor hubs with low energy levels. The source hub sends the message to neighbouring hubs, then move to the following neighbouring hub.

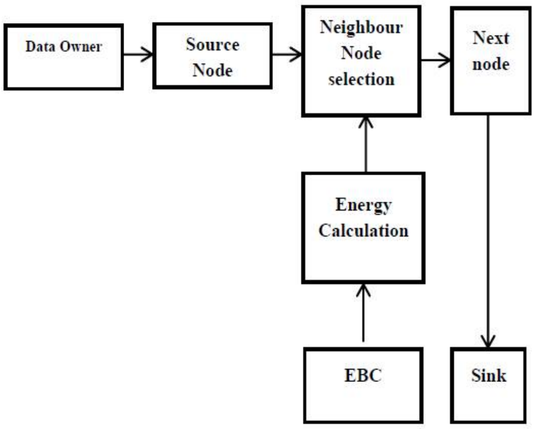


Fig: 4.1 overview of the system

The Fig 4.1 demonstrates that, the information is received by the destination node from the source node in view of the neighbour’s node choice. The EBC is the Energy Balance control; it is utilized to figure the energy. The energy is ascertaining taking into account the EBC algorithm. To start with select the neighbouring hub for message forwarding. On the off chance that the node/hub has the most elevated hub implies select that hub. The sink hub has the data about the whole hub, that data is put away to the sink hub. The source hub, sends the message to neighbouring hubs, then move to the following neighbouring hub. At long last the message is send to sink hub. In remote sensor network, sink hub has the all hub data. The EBC strategy is utilized to figure the energy for the sensor hub.

4.5. Modules Description:

There are mainly three modules considered in this project:

1. Shortest Path Distribution.
2. Energy Balance Routing.
3. Secure Routing Using CASER.

i. 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.

ii. 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. 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 A. The CASER path selection calculation is derived by the equation,

$$\varepsilon_a(\mathrm{A})=\frac{1}{\|N_A\|}\sum_{i\epsilon N_A}\varepsilon_{r_i}.$$

Here ε is a parameter utilized for the Energy Balanced Control. And after that the term α used to signify testing proportion. On the off chance that the α quality is most extreme means there is no shortest path in that hub.

iii. **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$\beta\epsilon[0,1]$, carried in each message.

V. SECURE ROUTING STRATEGY

In the previous section, we only described the shortest path routing grid selection strategy. However, in CASER protocol, we can support other routing strategies. In this section, we propose 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.

VI. NETWORK SIMULATOR 2(NS2)

Network simulator (version2) is commonly known as NS2. NS2 is an event driven simulation tool. The dynamic nature of common networks is studied using NS2 and simulations of wired and wireless network function are done by NS2. NS2 was evolved in 1989, because of its flexibility and modular nature it is very much used in many network researches.

6.1. Basic architecture:

The basic architecture of NS2 is as shown in the fig-.6.1. NS2 provides executable command ns to the users.

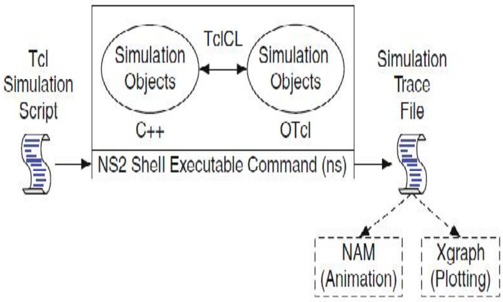


Fig: 6.1 Basic architecture of NS2

NS2 basically consist of 2 key languages: C++ and Object-oriented tool command language (OTCL). The C++ defines the internal mechanism of the simulation objects hence it is known as backend.

The OTCL sets up the simulation by assembling and configuring the objects. Also the OTCL starts scheduling discrete events. OTCL is known as the frontend the TclCL is used to link C++ and OTCL. The variables in OTCL are referred as handles. This handle is a string and do not contain any function. In OTCL domain a handle is a frontend and provide interaction between users and OTCL objects.

In OTCL domain the procedure and variable are called as instance procedure (intprocs) and instance variable (intvars).

A large number of built-in C++ objects are provided by NS2. These C++ objects can be used to set up a simulation. After simulation the outputs of NS2 are either text-based or animation-based simulation results. In order to interpret the simulation results graphically and interactively, the tools such as NAM that is network AniMator and XGraph are used.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

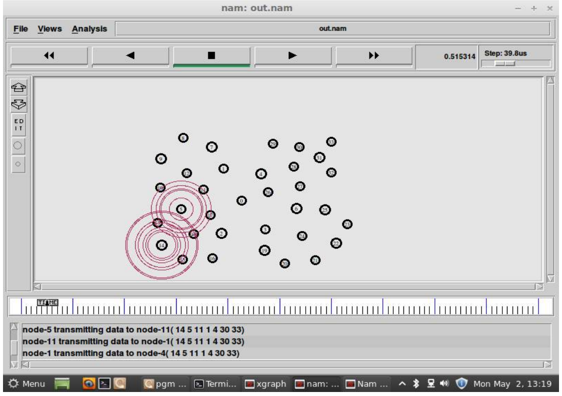
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

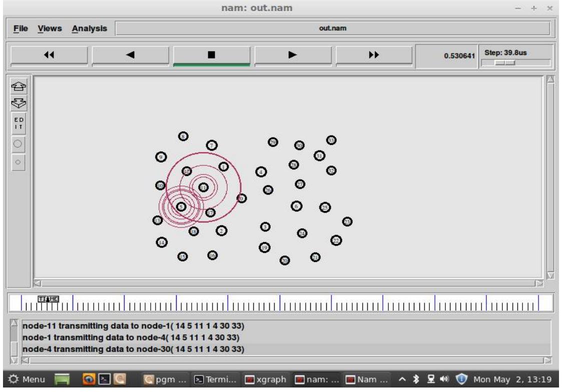
VII. EXPERIMENTAL RESULTS

This model is coded in NS2 and is made run in VMware workstation. 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.
We conducted simulations using OPNET to compare the message delivery ratio of uniform energy deployment and non-uniform energy deployment for different a values when b ¼ 0.



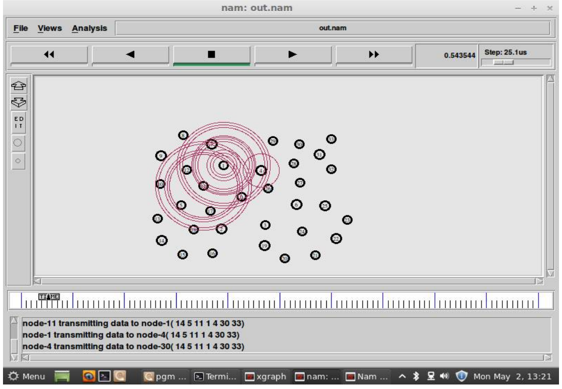
```
node-5 transmitting data to node-11( 14 5 11 1 4 30 33)
node-11 transmitting data to node-1( 14 5 11 1 4 30 33)
node-1 transmitting data to node-4( 14 5 11 1 4 30 33)
```

Fig: 7.1 routing from the source node 14 to the nearest node 5.



```
node-11 transmitting data to node-1( 14 5 11 1 4 30 33)
node-1 transmitting data to node-4( 14 5 11 1 4 30 33)
node-4 transmitting data to node-30( 14 5 11 1 4 30 33)
```

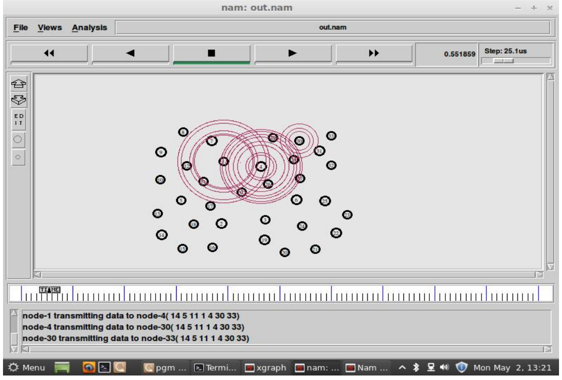
Fig: 7.2 routing from node 5 to node11



```
node-11 transmitting data to node-1( 14 5 11 1 4 30 33)
node-1 transmitting data to node-4( 14 5 11 1 4 30 33)
node-4 transmitting data to node-30( 14 5 11 1 4 30 33)
```

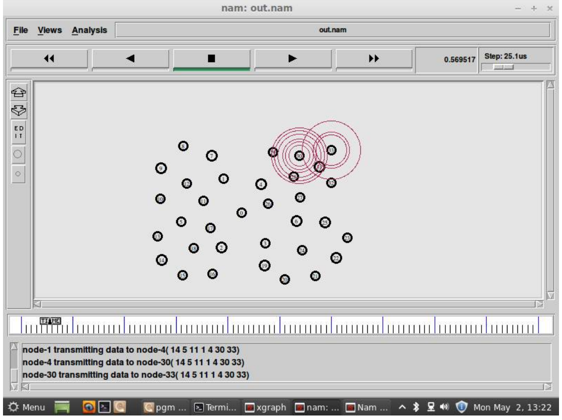
Fig: 7.3 routing from node11 to node1

DOI: 10.15680/IJIRCCE.2016. 0404349



```
node-1 transmitting data to node-4( 14 5 11 1 4 30 33)
node-4 transmitting data to node-30( 14 5 11 1 4 30 33)
node-30 transmitting data to node-33( 14 5 11 1 4 30 33)
```

Fig: 7.4 routing from node 4 to 30



```
node-1 transmitting data to node-4( 14 5 11 1 4 30 33)
node-4 transmitting data to node-30( 14 5 11 1 4 30 33)
node-30 transmitting data to node-33( 14 5 11 1 4 30 33)
```

Fig: 7.5 routing from node 30 to node 33

The above results are determined for energy balanced control. Here the node 14 is assigned as the source node and the node 33 is selected as the destination in order to exchange the information.

The seleted path for this particular transmission is (14 5 11 1 4 30 33). From node 14 the nearest node with high energy level is selected i.e., node 5 and the data is transmitted to the node 5. Then from node 5 the nearest node is seletced i.e., node 11 and the data is transmitted. Likewise, node 1, node 4, node 30 and the destination i.e., node 33 is provided with the imformation.

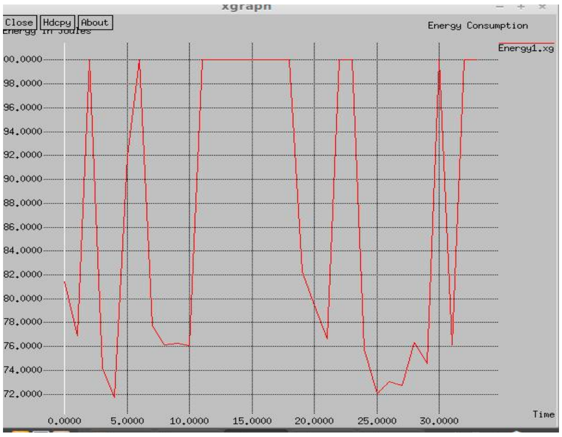


Fig7.6 Energy level depletion using random walk strategy

Figure 7.6 shows a graph for energy depletion in random walking process. As the number of hops is more the energy gets depleted more. As the number of the nodes increases for each hop the energy is consumed and by the time the destination node is detected there will be very less amount of energy available. Thus the energy depletes fast.

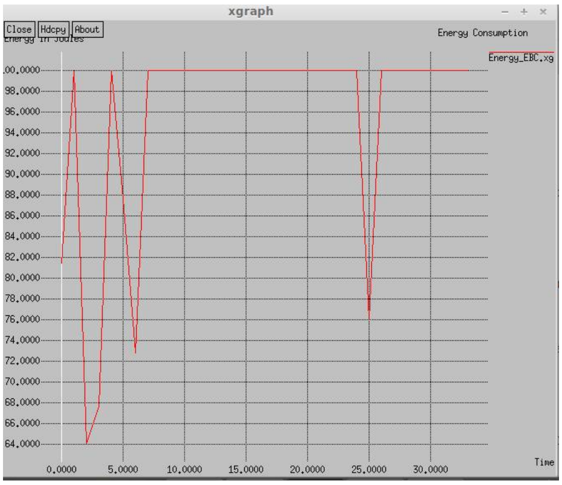


Fig 7.7 Energy level depletion using energy balance control scheme

When compared to the random walking strategy the energy balance control scheme consumes less energy as the number of nodes used to transmit the data is less. Hence energy depletion is reduced in this scheme.

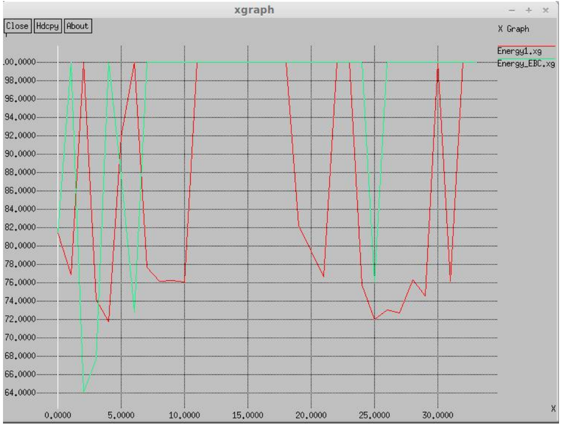


Fig 7.8 Comparison of energy depletion between energy balance control strategy and random walking

Here node 0 is taken as the source and node 5 is considered as destination in both the cases. In energy balance control scheme the number of hops is less and hence the energy depletion is less. Therefore a balanced energy strategy is taken into consideration and the lifetime of the senor is optimized. In random walk process the number of hops is more when compared to the energy control crisis. Hence the energy level drastically decreases and the life time of the sensor also decreases.

The figures show the energy depletion level of each of the strategy and the comparison between them.

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 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 proposed 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.

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 Distributed System, 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 Conference Computer Communication Mini-Conference, 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 Annual International Conference Mobile Computer Network, 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 Annual International Conference Mobile Computer Network, 2000, pp. 120–130.

[6] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad-hoc routing,” in Proc. 7th Annual ACM/IEEE Int. Conference Mobile Computer Network, 2001, pp. 70–84.

[7] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,” Computer Science Department, 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,” Computer Science. Department, University Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729, April. 2000.

[9]M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in Proc. IEEE 27th Conference Computer Communication, April. 2008, pp. 51–55.

[10] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-location privacy in sensor network routing,” in Proc. 25th IEEE Int. Conf. Distributed Computer System., June. 2005, pp. 599–608.

[11] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attack and defense strategies,” IEEE Network., volume. 20, no. 3, pp. 41–47, May/June. 2006.

[12] lifetime optimization and security in wsn Using e-caser protocol Veena V.K , S.Subbulakshmi Department of Electronics and Communication Engineering Valliammai Engineering College, Kattankulathur , Chennai, Tamilnadu, India. International Journal of Advanced Engineering and Global Technology Vol-03, Issue-12, December 2015

DOI: 10.15680/IJIRCCE.2016. 0404349