Optimizing the Network Lifetime and Improving the Network Security in Wireless Sensor Network

B.DIVYA, V.GOUTHAM REDDY

1M. Tech Student, Department of IT, Joginpally B R Engineering College, Village Yenkapally, Mandal Moinabad, District Ranga Reddy, Telangana, India

2Assistant Professor, Department of IT, Joginpally B R Engineering College, Village Yenkapally, Mandal Moinabad, District Ranga Reddy, Telangana, India

Abstract— Now a days, wireless networks are facing variety of drawback to transfer the information from source to destination through the varied routings. In that two major problems are extremely impact on networks those are network lifespan and security. Therefore, lifespan improvement and security are the most difficult design problems during this paper. To realize these two challenges for the first time we tend to projected (CASER) Cost-Aware Secure Routing protocol throughout this paper. According to this paper, in existing we tend to used uniform energy preparation at intervals the networks. Through this uniform energy preparation strategy, network lifespan reduced extraordinarily. For that in our protocol we offer non-uniform energy preparation strategy. Basically, our protocol works through two adjustable parameters that are 1) Energy Balance control (EBC) 2) Random Walking. Our protocol can considerably improve the network lifespan and security.

Index Terms--CASER, Energy Balance Control, Random Walking, Energy Consumption;

I. INTRODUCTION

WSN is a wireless network consisting of spatially distributed autonomous devices exploitation sensors to observe physical or environmental conditions. A Wireless Sensor Network (WSN) system incorporates an access that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol you choose depends on your application necessities the Wireless device networks (WSN), typically known as wireless sensor and mechanism networks (WSAN), the subsequent benefits of Wireless sensor Network applications for areas together with health care, utilities, and remote observation the recent technological advances build wireless sensor networks (WSNs) technically and economically doable to be wide used in every military and civilian application, like observance of shut conditions related to the setting, precious species and important infrastructures. A key feature of such networks is that each network consists of a large vary of unbound and unattended sensor nodes. These nodes usually have very restricted and non-replenish ready energy resources, that makes energy a very necessary design issue for these networks. Routing is another very difficult style issue for the WSNs. A properly designed routing protocol mustn't only guarantee high message delivery ratio and low energy consumption for message delivery, but collectively balance the complete sensor network energy consumption, and thereby extend the device network life. CASER protocol has two major advantages: (i) it ensures balanced energy consumption of the complete device network so as that the lifetime of the WSNs is also maximized. (ii) CASER protocol supports multiple routing methods supported the routing
desires, together with fast/slow message delivery and secure message delivery to forestall routing trace back attacks and malicious traffic electronic countermeasures attacks in WSNs. An efficient and a non-uniform energy preparation system to optimize time period and message delivery ratio below a same energy resource and a security demand it also can offer a quantitative security analysis on the projected routing protocol. It will offer an honest trade-off between the routing potency and therefore the energy balance, and may considerably enhance the time period of the device networks all told directions. For a non-uniform energy preparation, to maximize the time period and therefore the most range of messages that may be delivered by over four times by an equivalent assumption. To induce a high message delivery ratio whereas preventing the routing trace back attacks.

II. RELATED WORK

A wireless sensor network includes a massive amount of un-tethered and unattended sensor nodes. These nodes typically have very restricted and non-replenishable energy resources, that makes an energy a most significant design drawback for these networks. Routing could be a different terribly difficult style limitation for WSNs. A properly designed routing protocol should not be best confirm excessive message provide ratio and low energy consumption for message provide, however in addition steadiness the whole detector network power consumption, and thereby lengthen the sensor community lifespan. Additionally, the aforementioned problems, WSNs rely upon wireless communications that is by exploitation nature broadcasting. It is a lot of at risk of protection assaults than its wired counterpart as a result of lack of a physical boundary. In exact, within the wireless sensor domain, any person with an applicable wireless receiver will monitor and intercept the sensor network communications. The adversaries could use costly radio transceivers, powerful workstations and interact with the community from a distance since they are not restrained to creating use of detector community hardware. It is possible for the adversaries to perform electronic countermeasures and routing mention back assaults. whereas geographic routing algorithms have the advantages that every node simplest needs to preserve its neighboring data, and provide a much bigger effectively and a larger quantifiability for enormous scale WSNs, these algorithms might attain their neighborhood borderline, that is ready to impact in useless end or loops. Our broad OPNET simulation results exhibit that CASER will furnish best power balance and routing safety it is additionally established that the projected comfortable routing will expand the message delivery magnitude relation owing to diminished dead ends and loops in message ahead. The most drawbacks of existing system are: It cannot guarantee balanced energy consumption of the complete sensor network in order that the lifespan of the WSNs are often maximized. The secure message delivery does not to prevent routing trace back attacks and malicious traffic electronic countermeasures attacks in WSNs. The energy consumption is severely disproportional to the uniform energy deployment for a given networking topology that greatly reduces the lifespan of the sensor networks. During this paper, for the primary time, we tend to propose a secure and efficient cost Aware SEcure Routing (CASER) protocol that may address the energy balance and also the routing security at an equivalent time in WSNs. In CASER protocol, each sensor node needs to manage the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Exploitation this data, each sensor node can manufacture variable filters support the expected style trade-off between security and efficiency. The quantitative security analysis demonstrates the projected algorithm can defend the source location information
from the adversaries. Our thorough OPNET simulation results show that CASER can supply excellent energy balance and routing security. It’s in addition incontestable that the projected secure routing can increase the message delivery quantitative relation attributable to reduced dead ends and loops in message forward.

### III. FRAME WORK

In this paper, we tend to design a protocol i.e., CASER protocol. To use this protocol within the wireless sensor network at first we want to design the network. In figure1, we tend to consider that in our network we have more number of sensors and one sink node. During this network are going to be divided as grids. In every grid equivalent sensor nodes are deployed. From the figure1, we have four grids and in every grid have five sensor nodes. For complete network we have only single sink node.

It means that the sink node is simply destination for all sensor nodes. The data of the sink node is created public. For security functions, each message will be assigned a node identity corresponding to the situation the place this message is initiated. To prevent adversaries from raising the source location from the node identity, a dynamic id will be used. The content of each message may be encrypted making use of the key shared between the node/grid and the sink node. We tend to additionally anticipate that each sensor node is conscious of its relative neighborhood within the sensor area and has competencies of its instant adjacent neighboring grids and their vigor levels of the grid. The understanding concerning the relative area of the sensor domain might also be broadcasted at intervals the network for routing data replaces. Routing strategies in CASER in this protocol, two types of strategies are there: 1. deterministic Routing Strategy, 2.Random Walk Routing Strategy

**deterministic Routing:** really, the CASER protocol works supported two adjustable routing parameters like follows: 1. Energy Balance control (EBC), 2.Random Walk in settled routing, we tend to use the EBC parameter. During this strategy we tend to implement the non-uniform energy readying strategy. During this strategy, initially all sensor nodes have an equivalent energy and once your time they lose few quantity of energy. Remaining energies are we need to calculate first. After that we tend to should select the candidate grids.

Candidate grids means that based on calculated energy levels of sensor nodes; in each grid we have one high energy level node. We tend to choose that node to routing which node grid is referred to as a candidate grid. Supported selected candidate grids we tend to formulate a shortest path. Through that shortest path we tend to are sending the information. Finally, we are able to maintain the energy levels of the sensor nodes within the network. Like this, we are able to optimize the network life with efficiency within the wireless sensor networks. Security in CASER Protocol: In random walking parameter, CASER protocol sends the messages
with secure. Once sender node sends the information to sink node, throughout transmission variety of attacks square measure might occurred. So, during this protocol we tend to implemented Random walking strategy. To produce the safety we tend to choose the random walk routing strategy. It not only provides the protection to the node however additionally it managed the energy levels. In random walk routing strategy, after we send the data through the shortest path it will not shows the sender node to protect the node details and corresponding data from the hackers. It simply hides the particular sender node details and it displays the nearest node of the sender node as a sender node. By implementing likewise, there is no possibility to the attacker to induce the sender node details if we tend to observe the particular sender node are going to be located in shaded space and nearest node displayed as sender node. Here, based on node distance we are able to estimate that node is nearest to the sender node. Like this we are able to forward the messages from sender node to the sink node. During this paper, initial we tend to control the energy levels of the sensor nodes. When we are managed the sensor nodes energy levels within the network, then automatically, we tend to optimize the network lifespan. If network life is increased, then we are able to increase the high message delivery ratio within the wireless detector networks. Through the random walk strategy we are able to achieve the security aspect additionally at a time within the routing.

**IV. EXPERIMENTAL RESULTS**

In our experiments, any number of users can create the network in that network to give the node size means number of nodes to be created in the network for example to enter 20 nodes and we can also select the routing type like Deterministic routing (energy balance control EBC) or secure random walk (probabilistic based random walking) after selecting the routing type the network simulation screen will be displayed in that network simulation screen the network will be created 20 nodes the 20 nodes will be divided into 4 sections they are forward, backward, upward and downward sections to shown in below screen

![Network Simulation Screen](image)

After that to select any sender node here for every time instead of sending the data from a sensor to the base station from a single section, we can make use of other sections also to reduce energy consumption of that particular node after that to see each node energy level after that same as to select another routing type to perform same operation and we can also see the each node energy level to shown in below chart

![Energy Level Chart](image)

We can observe that energy level chart to see the energy levels on each and every node. Through our implementation we can to send the data in best routing path and also we can increase the node energy at lower cost then compare to current techniques.

**V. CONCLUSION**

From this paper, we tend to present a secure and efficient cost Aware SEcure Routing (CASER) protocol for Wireless sensor Networks to reduce the energy consumption and increase lifetime of networks. CASER
is flexible to support many routing ways in message forwarding to increase lifetime and, whereas increasing the routing security. Both the theoretical analysis and simulation results prove that CASER has excellent routing performance if we tend to consider the energy balancing and a routing path distribution for a path security. We have additionally planned a non-uniform energy deployment approach to maximize the sensing element network lifespan. Analysis and Simulation results show that we will extend the lifespan and the number of messages to be delivered by the non-uniform energy deployment.

REFERENCES