International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Optimizing Networking Lifetime and Improving Security for Wireless Sensor Network through an Efficient Routing Protocol

N. Mahesh , K.Maheshwari Devi , K. Ashok Babu
M.Tech in Digital Electronics & Communication Systems, Sri Indu College of Engineering & Technology, Sheriguda, Ibrahimpatnam, RR.Dist. HYD
Assistant Professor, Dept of ECE Sri Indu College of Engineering & Technology, Sheriguda, Ibrahimpatnam, RR.Dist. HYD
Professor & HOD Dept of ECE Sri Indu College of Engineering & Technology, Sheriguda, Ibrahimpatnam, RR.Dist. HYD

ABSTRACT— *In wireless sensor networks, we have two major challenges such as network lifetime optimization and another is security. Traditional networking protocols are cannot provide the complete security for the nodes in the network. The existing protocols are suffering from network lifetime problem which means no protocol can control the energy levels of the network nodes. While routing, if any node may loss energy levels then the network failures may occurred as well as data loss also occurred. Through this high energy consumption, the packet delivery ratio also reduced. And in this paper, we focused on traceback attacks on the wireless sensor networks. To overcome these conflicting issues, we propose an energy efficient and Cost-Aware SEcure Routing (CASER) protocol. By using this protocol, we can optimize the network lifetime and also we can improve the network security in wireless sensor networks. The simulations are performed on the NS2 simulator. Through the simulation, we can prove that our proposed protocol is energy efficient and secure protocol.*

Keywords: Wireless Sensor Network, Traceback Attacks, Network lifetime and Network Security

1. 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 manner, a malicious node may arrive the network. Due to the wireless strategy, snooping can be easily achieved in this environment which creates the network accessible 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 has 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 are 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. Cost-Aware Secure Routing (CASER) protocol for WSNs to steadiness the energy consumption and develop network lifetime. Our analysis will showing that we are able to develop the lifetime and the number of messages that may be delivered below the non-uniform energy deployment by way of greater than four occasions. CASER supports secure delivery, to hinder routing trackback attack and malicious site visitors jamming attack in wireless Sensor communication.

2. RELATED WORK

Y. Li, J. Li, J. Ren, and J. Wu were proposed an efficient Source Anonymous Message Authentication scheme (SAMA) and it worked based on Elliptic Curve Cryptography (ECC). While ensuring message sender privacy, proposed scheme can be applied to any messages to provide hop-by-hop message content authenticity without the weakness of the built-in threshold of the polynomial-based scheme.

P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia described algorithms for routing, broadcasting, and geo-casting in unit graphs. The algorithms do not require duplication of packets, or memory at the nodes of the graph, and yet guarantee that a packet is always delivered to (all of) its destination(s). There are several open problems and directions for future work in this area. One such direction is the extension of this work to dynamically changing networks. Although it is possible to extend our algorithms with the hope of handling dynamically changing networks, it is not at all clear what is a reasonable (mathematical or simulation) model under which to study these modified algorithms. Akshay Dubey, Medhavi Shriwas proposed an enhanced performance of routing protocol in relations of energy consumption. This routing is controls a route only must shortest time, but since the control packets and routing are not applied, there is a waste of network resources. The routing information stored and maintained by this proposed protocol. In the high-speed dynamic network, it shows higher performance. The main suggestions in works are offered and the main methods accepted for ad-hoc energy consumption decrease is clarified. The works offered are

characterized by the environment of their performance: proactive, reactive and hybrid ones. In various cases, it is problematic to compare them directly since each process has a dissimilar aim with different moulds and employs different means to complete the goal.

3. FRAMEWORK

A. System Design

In this paper, we design a protocol i.e., CASER protocol. To apply this protocol in the wireless sensor network initially we need to design the network. We consider that in our network we have more number of sensors and a single sink node. In this network will be partitioned as grids. In each grid equivalent sensor nodes are deployed. From the figure, we have four grids and in every grid have five sensor nodes. For complete network we have only single sink node.

It means the sink node is only destination for all sensor nodes. The data of the sink node is made public. For security purposes, every message can be assigned a node identity corresponding to the location the place this message is initiated. To prevent adversaries from improving the source location from the node identity, a dynamic id can be utilized. The content of each message can also be encrypted making use of the key shared between the node/grid and the sink node. We also anticipate that every sensor node is aware of its relative vicinity within the sensor area and has competencies of its instant adjoining neighboring grids and their vigor levels of the grid. The understanding concerning the relative area of the sensor domain could also be broadcasted within the network for routing data replace.

B. Routing Strategies in CASER

In this protocol, two types of strategies are there:

1. Deterministic Routing Strategy
2. Random Walk Routing Strategy

Deterministic Routing:

Actually, the CASER protocol works based on two adjustable routing parameters such as follows:

1. Energy Balance Control (EBC)
2. Random Walk

In deterministic routing, we use the EBC parameter. In this strategy we implement the non-uniform energy deployment strategy. In this strategy, initially all sensor nodes have the same energy and after some time they lose few amount of energy. Remaining energies are we need to calculate first. After that we must select the candidate grids.

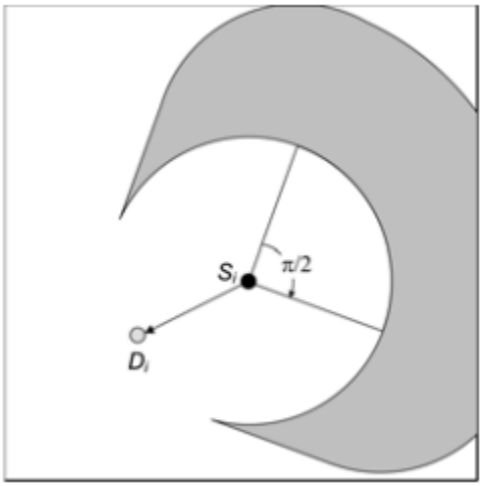


Figure1: Deterministic Routing

Candidate grids means based on calculated energy levels of sensor nodes; in every grid we have one high energy level node. We select that node to routing and that node's grid called a candidate grid. Based on selected candidate grids we formulate a shortest path. Through that shortest path we are sending the data. Finally, we can maintain the energy

levels of the sensor nodes in the network. Like this, we can optimize the network lifetime efficiently in the wireless sensor networks.

C. Security in CASER Protocol

In random walking parameter, CASER protocol sends the messages with secure. When sender node sends the data to sink node, during transmission number of attacks are may occurred. So, in this protocol we implemented Random walking strategy. To provide the security we select the random walk routing strategy. It not only provides the security to the node but also it managed the energy levels.

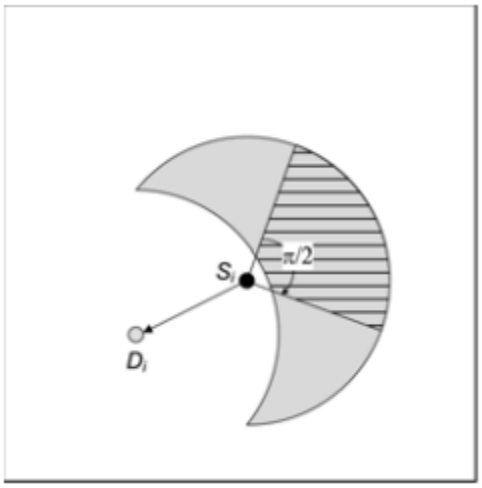


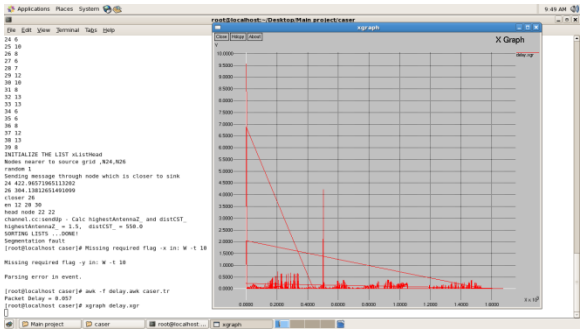
Figure2: Random Walking

In random walk routing strategy, when 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 just hides the actual 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 get the sender node details.

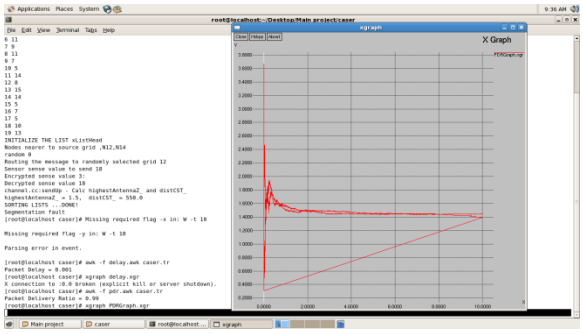
If we observe in figure2, the actual sender node will be located in shaded area and nearest node displayed as sender node. Here, based on node distance we can estimate which node is nearest to the sender node. Like this we can forward the messages from sender node to the sink node. In this paper, first we control the energy levels of the sensor nodes. When we are managed the sensor nodes energy levels in the network, then automatically, we optimize the network lifetime. If network lifetime is increased, then we can increase the high message delivery ratio in the wireless sensor networks. Through the Random walk strategy we can achieve the security aspect also at a time in the routing.

4. EXPERIMENTAL RESULTS

In this experiment, we used centos for NS2 Simulations. The CASER protocol can used the two parameters such as energy parameter represents with 1 and security parameter represents with 0.



In the simulation, we can transfer the message from source to sink node in the network. We can view the delay among the source and sink node to transfer data.



We need to achieve the high message delivery ration using CASER protocol. The above graph described about the packet delivery ratio. From the experimental results, we can proved that we achieved the high message delivery ratio with secure.

5. CONCLUSION

In this paper, we proposed a CASER protocol. The main aim of this protocol is to optimize the network lifetime as well as provide security to the network. To achieve this aim, this protocol worked through two adjustable parameters such as follows 1) Energy Balance Control and 2) Random Walk. Eventually, we achieved the network lifetime optimization along with security and we achieved high message delivery ratio. We proved our aim by our simulation results.

REFERENCES

[1] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design ofsource-location privacy schemes for wireless sensor networks,"IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul.2012.

[2] 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.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. 6th Annu. Int. Conf. MobileComput. Netw., New York, NY, USA, 2000, pp. 243–254.

[4] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "Ascalable location service for geographic ad hoc routing," in Proc.6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 120–130.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energyconservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEEInt. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

[6] 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, LosAngeles, CA, USA, Tech. Rep., May 2001.

[7] 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. 00-729, Apr. 2000.

[8] . Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7thACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing withguaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int.Workshop Discrete Algorithms Methods Mobile Comput. Commun.,1999, pp. 48–55.

[10] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing withguaranteed delivery in ad hoc wireless networks," in Proc. 3rdACM Int. Workshop Discrete Algorithms Methods Mobile Comput.Commun., Seattle, WA, USA, Aug. 1999, pp. 48–55.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

N. MAHESH[1,] Pursuing M.Tech in Digital Electronics & Communication Systems Sri Indu College of Engineering & Technology, Sheriguda,

K. MAHESHWARI DEVI[2,]

Currently working as Assistant Professor, Dept of ECE, Sri Indu College of Engineering & Technology, Sheriguda,

K. ASHOK BABU[2,]

Currently working as professor & HOD, Dept of ECE, Sri Indu College of Engineering & Technology, Sheriguda,