VOL. 10, NO. 10, JUNE 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURITY AND ENERGY EFFICIENCY BASED EC-MAC PROTOCOL FOR SENSOR WIRELESS NETWORKS

R. G.Nishaa and P. Latha
Department of Information Technology, Saveetha Engineering College, Thandalam, Chennai, India
E-Mail: nisha.rajendran21@gmail.com

ABSTRACT

Security as well as energy consumption is the main components of wireless sensor network. Sensor node has the main functional component present in the WSN. In order to improve the efficiency of energy consumption, enhanced version of (EC-MAC) is proposed. Emergency Code-Medium Access Control (EC-MAC) is responsible for emergency purposes. The proposed MAC protocol is designed using the Carrier Division Multiple Access (CDMA) mechanism. CDMA can be used to enable multiple users to access shared medium without interference. The main resource of EC-MAC protocol is well suited to change the topology in MAC protocol during emergency mode. The MAC behaviour changes during the change in the topology and may inject the data detection. In order to address these issues, Fuzzy-Concealing Sink Hole (F-CSH) may be used to find the location of the main sink using the fake sink holes to anticipate the traducer to turn the network to deplete the node energy and abunding the network with bogus data. RSSI may be used to estimate the distance between the two nodes during the data transmission.

Keywords: energy-efficiency, MAC protocol, security, fake data, delivery ratio, RSSI, CDMA.

1. INTRODUCTION

Now a days most way of communicating, broadcast the message through the wireless sensor networks. WSN have several characteristics such as energy efficiency, security, optimization and load balancing etc. The main objective of sensor networks is to sense the node and transmitting the data with high delivery ratio and low latency. Major application of sensor network such as detects earth quake, machinesurvillence and preventive maintenance, medicine and health care, logistics. Sensor network can be divided in to two types: wired and wireless networks. Wireless sensor has consumed more energy compared to the wired networks. MAC protocol present in the wireless sensor networks are used for analyzing the process and increase the capacity of the nodes, packets. It act as main functional component in the networks. The proposed system may overcome the large amount of energy consumption during transmitting data. Usage of energy in sensor nodes is high for increasing the performance analysis. In existing system, several Z-mac, ER-mac protocols is used to increase the energy efficiency. Compare to all existing protocols, proposed system have high delivery ratio, low latency and high energy efficiency. In order to increase efficiency, we focus also security to the networks. Security is added to the proposed network; prevent the attacker to restrict the network with fake data. Security is the important aspects present in the networks. Several algorithms can be used and discovered for high security. In recent years WSN have high security focused on data transmission. But earlier work can have lack of security and low delivery ratio. The proposed can analysis security added with energy efficiency. RSSI can be used to measure the distance between the two nodes and detect the fake nodes present in the topology. F-CSH (fuzzy concealing sink holes) can be used to detect the fake sink hole by using fuzzy score or RSSI.

2. RELATED WORKS

In this section, overview of existing energy saving MAC protocol for WSN and detection of malicious node is explained.

2.1 ER-MAC

ER-MAC aims to explain ER-MAC protocol to cope with heavy traffic, robust adaptation to changes in the topology, packet priority and support fairness. ER-MAC using the TDMA approach to schedule collision-free slots. It offers a synchronized and loose slot structure, where nodes can modify their schedule locally. This allows nodes to join or leave the network easily. Due to these changes result in the intrusion of fake data. Autonomous switching the network can lead to security attacks in the nodes.

2.2 Z-MAC

An efficient hybrid protocol Z-MAC is the combination of TDMA and CSMA. It utilizes CSMA in low channel combination and switch to TDMA mode in high channel contention. Z-MAC does not perform well under high traffic load. A hybrid protocol has initial slot assignment. It does not manage the high traffic load occured. Highcontention in Z-MAC can have hidden termination problem while transferring the messages by using ECN (Explicit Contention Notification).This paper proposes few enhancements to achieve the better performance.

2.3 MAX-MAC

Max-mac has an energy efficiency MAC protocol in the wireless sensor networks. The aim of MAX protocol is minimize energy consumption in the sensor networks. Max has higher energy efficiency in the performacevalue. The main issue is collision occur in scheduling. It only focused on energy consumption and there is no scheduling or collsion free algorithm used.

2.4 Malicious data in sink node

In emergency application, security is the important aspect in the networks. The attacker may switch the network with emergency and [1] also fill the networks with fake data in high priority packets. The fake sink hole present in the gathering tree, it can be detected by using concealing sink node of the tree. The distance between the sink node can be detected by using [6] or fuzzy score function.

3. EMERGENCY CODE MEDIUM ACCESS PROTOCOL (EC-MAC)

The proposed EC-MAC protocol for wireless sensor network will increase the energy efficiency and delivery ratio. CDMA mechanism is used to schedule the data without collision during emergency mode. The purpose of using CDMA is transmission of data at a time with same link estimation.

3.1 EC-MAC protocol for data communication

Initially, EC-MAC protocol forms the basic structure of data-gathering tree. The tree is called as "Simple Emergency Data Transmitting" (SEDT).SEDT structure is mainly based on bottom up approach []. SEDT has one sind node and multiple parent and child node. Sink node is the main node to transmitting and control the data throughout the network by using TOPOLOGY-DISCOVERY.

1. source_ID is the sender of the message.
2. hop_count stores the number of hops to reach the sink.
3. original_parent_id stores the new parent ID of a node.
4. duplicate_parent_id stores a node's previous parent ID.

Topology Discovery is mainly focused on broadcast the message to its corresponding nodes. Nodes can be named as parent and children node. Duplicate node can be active during the emergency response and also message delivered to parent node. Nodes can send data by hop-count (one-hop and two-hop).

3.2 CDMA slot schedule

After topology discovered, CDMA start its schedule from the bottom (leaf node) to the top node (sink node).The message should be transmitting towards sink node from the leaf node. TDMA cannot be used to schedule data for exclusively large amount of data. CSMA/CA can be used to avoid collision. The feature beyond the CDMA is to transmit the data throughout the network with same link estimation.

3.3 RSSI based localization

The distance between two nodes will be measured by emerging the space between two nodes is detected using RSSI. Information between sink node and other nodes can be extracted using RSSI.

3.4 Malicious data detection using fuzzy rules

Fake node can be detected using Fuzzy Based Concealing Sink Node with Fake Holes (F-CSH).F-CSH is based on the concealing the location of the main sink using the elected fake sink holes by fuzzy score function. Fake Sink hole can be detected by using RSSI link estimation. In order to use this, to prevent the fake data entered in to the networks during emergency.

Fake Sink holes announcement

1. Compute and broadcast the fuzzy score.
2. The highest fuzzy score nodes will be the fake sink holes of the current round.
3. Other nodes, select their fake sink holes based on the fuzzy score or RSSI.

4. ANALYSIS OF EC-MAC

Overview of EC-MAC is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan to implement the process. This architecture describes the module of the system. Initially, data will be gathered from sensor nodes by the sink node. Nodes can transmit their data between them using topology. They are two modes of transmission: Normal mode and emergency mode. Both nodes have one-hop and two-hop count. Emergency mode is used to transmit data immediately. Emergency mode schedules their process using CDMA for mechanism. CDMA is used by the sensor node to transmit the data. Security is added to this process, since change of topology during emergency mode. F-CSH can be used to prevent the fake data. After delivering the packet with low latency, it can be detected for fake data. Finally EC-MAC have high energy efficiency with secured data transmission.

5. PERFORMANCE EVALUTION

5.1 Packet drop

EC-MAC protocol performance can be analysed based on packet drop. Packet drops occur due to traffic or interference present in the topology. Comparing to existing MAC protocol, performance of EC-MAC has more efficiency. In Figure-3 EC-MAC evaluates and determines its performance ratio. Performance can be analyzed based on the time taken to transmit the packets (X-axis) and number of packets dropped during transmission (Y-axis).

5.2 Packet delivery

Packet delivery is an important aspect in the data transmission. The proposed EC-MAC uses CDMA for scheduling the data with collision free slot that gives a high delivery ratio. Compare to existing MAC protocol EC-MAC have high delivery ratio shown in Figure-4.This graph shows the result of high delivery ratio obtained by using number of packets and time taken by a node.

5.3 Latency

Network connection speed can be determined by latency factor. Time taken to send the data by EC-MAC is low while using CDMA.CDMA schedule the packets based on high priority and low priority. This approach may help the node to transmit data with high speed. Reviewing the EC-MAC with existing MAC, EC-MAC has high speed networks shown in Figure-5.

5.4 High throughput

EC-MAC achieves high throughput efficiency minimize energy consumption. The proposed MAC have high throughput with successful message over communication channel. Number of data to be sent can be plotted in X-axis and time taken by a node can be measured in Y-axis.

6. CONCLUSIONS

In addition to adapting traffic and topology, proposed EC-MAC protocol will also reduce energy consumption. The topology is discovered by initiating the sink node to transmit the data. Topology will entered in to emergency mode, with the help of MAC, transmitting the data to the sink node that will produce low latency. Fake data may occur due to topology changes. To prevent an attacker entering into the node, Fuzzy-concealing sink hole (F-CSH) is used.

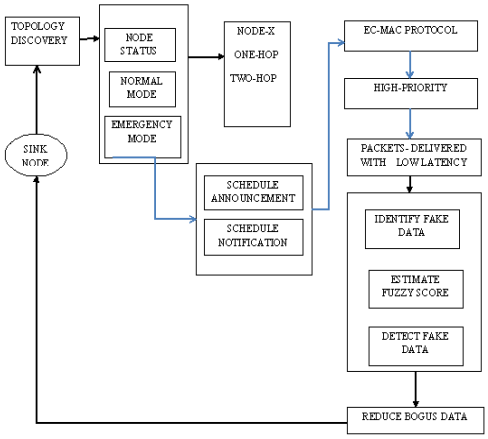

Figure-1. Overview of EC-MAC protocol communication.

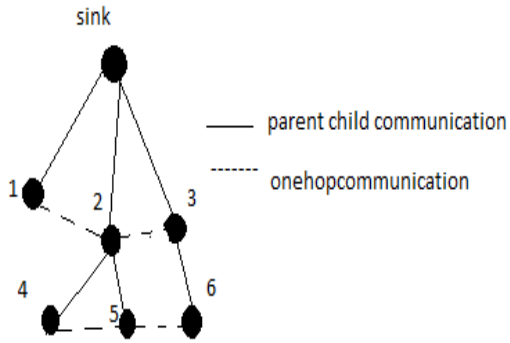

Figure-2. A data gathering tree.

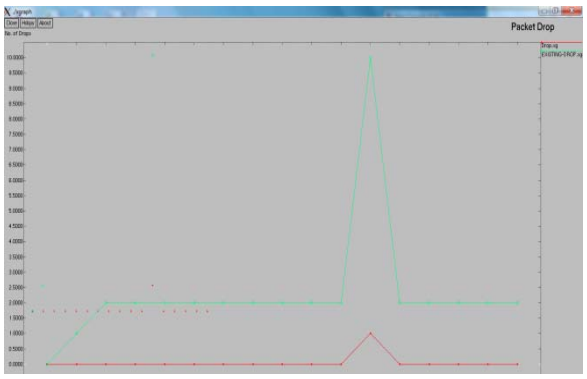

Figure-3. Packet drop.

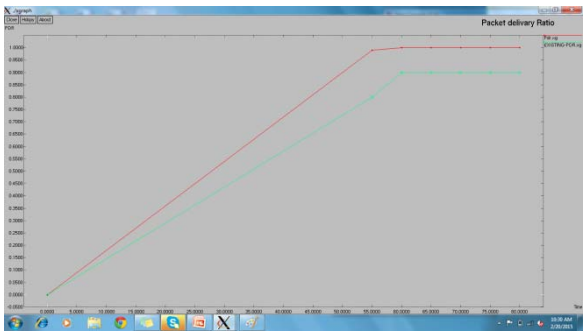

Figure-4. Packet delivery.

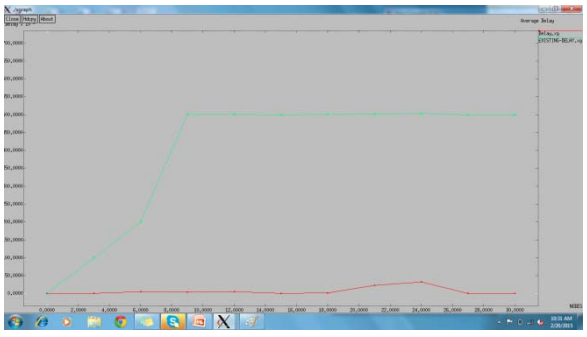

Figure-5. Packet average delay ratio.

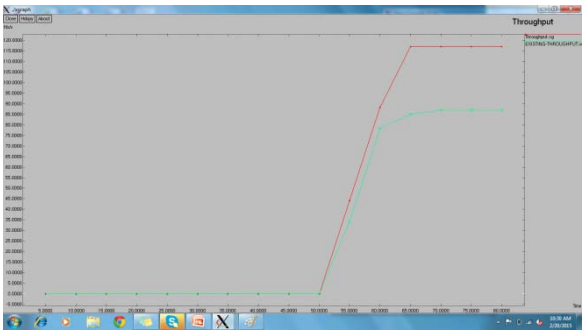

Figure-6. Packets with high Throughput.

REFERENCES

[1] Lanny Sitanayah, Cormac J. Sreenan, Kenneth N. Brown. 2014. "A hybrid MAC protocol for emergency response wireless sensor networks" in Mobile and Internet Systems Laboratory, University of cork, volume 21, 13 April 2014, pp. 77-95.

[2] Shoieb Arshad, Azzat Al-Sadi, Abdulaziz Barnawi. 2013. "Z-MAC: Performance Evaluation and Enhancements," in King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia, Volume 20, 2013.

[3] Kamal RahiniMaleskhan,Weihura Zhuang. 2014. "An Energy Efficient MAC Protocol For Fully Connected Wireless Ad Hoc Networks," in IEEE Transaction 08 October 2014, Volume 13, Issue 4. Bao Hua Liu, NirupamaBulusu, Huan Pham, Sanjay Jha, "CSMAC: A Novel DS-CDMA Based MAC Protocol for Wireless Sensor Networks".

[4] LujuanMa, Henry Leung, and Deshi Li. 2014. "Hybrid TDMA/CDMA MAC Protocol for Wireless Sensor Networks," JOURNAL OF NETWORKS, Vol. 9, No. 10, October 2014.

[5] Constaninos Marios Angellopulos, Sotris Nikoletsas. 2014. 'Wireless Energy Transfer in Sensor Networks with Adaptive Limited Knowledge Protocols,'19th IEEE Conference on Computer Communication, pp. 113-141.

[6] Forough Yaghoubi, Ali-AzamAbbasfar, Behrouz Mahan. 2014. 'Energy Efficient RSSI-Based Localisation for Wireless Sensor Networks,' IEEE Communication Letter, Vol. 18.

[7] Hurni .P, Braun .T, MaxMAC, 'A Maximally Traffic-adaptive MAC Protocol for Wireless Sensor Networks. 2010. 7th European Conf. Wireless Sensor Networks (EWSN'10), LNCS, Vol. 5970, pp. 289-305.

[8] Huanhuan Wang, Jianchen Wan, Ruyou Liu, 'A Novel Ranging Method Based on RSSI,' (2011), Proc. University of Electronics Science and Technology of China (UESTC), pp. 230-235.

[9] Kamal Rahimi Maleskshan, Yves Lostanlen, 'An Energy Efficient MAC Protocol for Fully Connected Wireless Ad Hoc Networks. 2013. IEEE Transaction on Wireless Communication.

[10] Krishan Kumar Raman, VP Singh, 'Transmission Energy Management for Wireless Ad-hoc Network. 2014. International Conference on Reliability, Optimization and Information Technology -ICROIT.

[11] Merhi. Z, Elgame. M, Bayoumi .M, 'EB-MAC an Event Based Medium Access Control for Wireless Sensor Networks,' IEEE Int'l Conf. Pervasive Computing and Communications (PerCom'09), pp. 1-6.

[12] Rini Van Solingen and K. Janani, 'Securing the Location Privacy in Wireless Sensor Networks. 2013. International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, pp. (1-4).

[13] Subodh Ku. Gond and Sai Prasad, 'Green Antenna and Radio over Fiber Technology for a Cellular Wireless. 2012. International journal of Engineering and Technology, Vol. 2.

[14] Taochun Wang, Xiaolin Qin and Liang Liu, 'An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks. 2013. International Journal of Distributed Sensor Networks, Vol. 2013, pp. 1-11.

[15] Valencic, Lebinac, Skendzic A, 'Developments and Current trends in Ethernet technology. 2013. IEEE conference Publications.