Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 6; October, 2014 pp. 13-18
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Comparative Analysis of Energy Efficient Secure MAC Protocols for Wireless Sensor Network

Balmukund Mishra[1], Yashwant Singh[2], Vandana Mohindru[3]

[1]M. Tech, Jaypee University of Information Technology, Waknaghat. HP
[2.3]Jaypee University of Information Technology, Waknaghat. HP, India

Abstract: **Wireless Sensor Networks (WSN) are practiced in many real life applications such as military, weather forecasting, medical, target spotting and tracking, etc. The sensor nodes are spread over the target area for the accumulation of data. The collected data further transmitted from one sensor node to other sensor node. WSN nodes have limited resources like energy, memory and processing capabilities. Efficient utilization of these resources is challenging task in WSN. MAC layer of wireless sensor nodes plays a vital role in WSN because most of the power is depleted at this layer due to collision in medium access and node synchronization.**

This paper presents a comparative analysis of all the existing WSN MAC protocol. The comparison is done on the basis of various parameters such as energy consumption, end to end latency, scalability, security from the outside attacker. Analysis of these MAC protocols will serve us in future detection as well as a selection of a protocol for a particular WSN application.

Keywords: **WSN, MAC, Energy inefficiency, network throughput, synchronization, collision, network delay.**

1. INTRODUCTION

Wireless sensor network is a kind of ad hoc network where sensor node may be deployed in remote, hostile environment, so power consumption and the security is the main issue in WSN. Lifetime of sensor node is directly dependent upon the battery lifetime or power consumption because changing the battery in a very short time is not possible in WSN. A very large number of applications are facilitated through WSN like weather forecasting, precision agriculture, environmental monitoring, intrusion detection, target tracking, etc. A major part of power is consumed in radio (transmitter and receiver), which is controlled by the MAC protocol [1]. MAC protocols are the protocols used at the link layer to provide access to the medium, scheduling, buffer management, and error control. The main goal in our MAC protocol design is to reduce energy consumption, while supporting good scalability and collision avoidance. . So the energy efficient MAC protocol will increase the lifetime of sensor networks up to a certain level. Security at Mac layer is another important concern because by attacking at a node, an attacker can waste the WSN node energy unnecessarily, steal, and interrupt data transmission. So for energy efficient MAC protocol, security is also very necessary.

In the first part of our paper we will describe the design challenges of MAC layer WSN and then attributes of good MAC protocols are described. In the next section we will classify the types of WSN MAC protocols with the help of a diagram. And then in the next part all the important energy efficient and secure MAC protocols are discussed in brief. After this we will try to differentiate all the energy efficient MAC protocol and will give a table based on attribute collision, overhearing, idle listening, latency etc. and then we will compare the protocols based on an application that is which type of protocol is good for which kind of application.

2. MAC PROTOCOL DESIGN CHALLENGES

Use of energy efficient, secure MAC protocol provides reliability and efficiency to the WSN. MAC is responsible for medium access, scheduling, buffer management and error control. The good MAC protocol is energy efficient, reliable, low rate of access delay, and high throughput. Energy efficiency is the most important because of low battery capacity and ad-hoc, unstructured deployment of WSN node in hostile environments.

2.1 Attributes of a Good MAC protocol

1) **Energy efficiency.** Large number of sensor nodes are deployed in the target region, which have limited battery and not possible to recharge or replace it. So it is necessary to use the energy efficient protocol at every layer.
2) **Latency.** All the data collected at a node are sent to the sink node so that immediate action should be taken a sink. Latency basically depends upon the traffic in the network, collision and bandwidth of the network.
3) **Throughput**. Throughput requirement is also dependent upon the application. Some sensor application requires more data for that application throughput should be high.

4) **Fairness:** it is necessary to ensure that the sink node is receiving data from at the node fairly in low bandwidth WSN.

5) **Security.** WSN MAC protocols need to secure for any application of WSN. The unsecure MAC protocol can cause to energy wastage.

2.2 Major Sources of energy Wastage in MAC Layer

- Major sources of energy wastage n WSN is a collision, exchange of control packets, Overhearing, and Idle listening [3].
- For the WSN handling of idle listening is more important because nodes are kept alive even when the node has neither data to send or receive.
- When developing a new protocol we have kept in mind about all these sources of energy wastage as well as the security level of the protocol.
- The attacker can make the protocol more than worse if not secure, by simply DOS (jamming) attack. So in spite protocol being energy efficient it must be secure enough to WSN attacks.
- We have been categorized the WSN MAC protocols in three parts; contention based, schedule based, and secure WSN MAC.

3. MAC PROTOCOLS CATEGORIZATION [FIGURE-1]

MAC protocols presented in the literature can be classified in two groups according to the approach used to manage medium access contention based and schedule based and a secure MAC protocol specifically designed to provide security at MAC layer protocols.

Before discussing energy efficient MAC protocols that are specifically designed for WSN, some Traditional MAC protocols like ALOHA, CSMA, and CSMA/CD are there in which it is important to understand the mechanism of CSMA here and the reason why it cannot be used directly in WSN.

3.1 CSMA Mechanism

Instead of using directly CSMA mechanism because of their disadvantage, high rate of collision, it is used in both contention based and schedule based protocols. In contention based protocol CSMA is used in basic data communication. Similarly in reservation based protocol slot requests are generally performed through CSMA.CSMA is a listen for transmit method. The functionality of CSMA are..

The node first listens to the channel for a specific time (IFS, inter frame space) and then work as follows

If the channel is idle the duration of IFS, the node may transmit the data.

If the channel becomes by during the IFS, the node defers the transmission and continues to monitor the channel until the transmission is over.

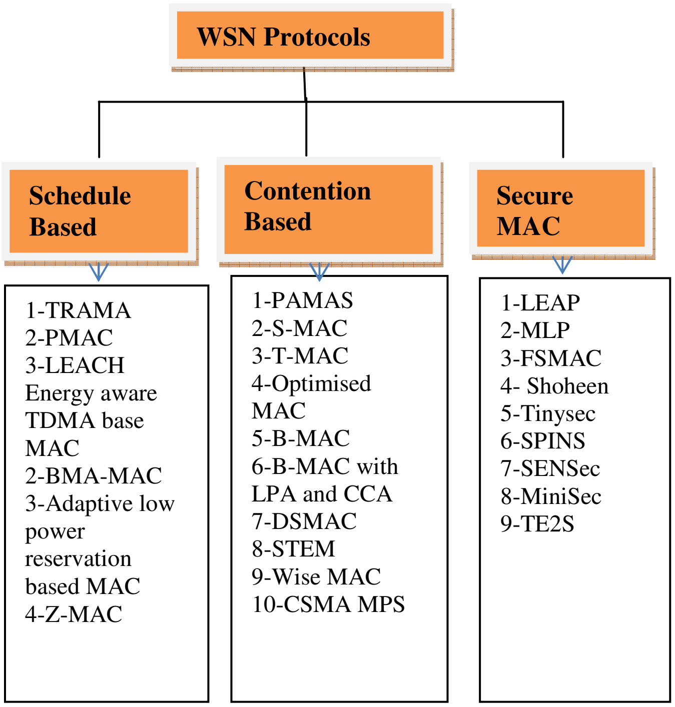

Fig.-1 MAC protocols categorization

3.2 Contention Based MAC Protocols

Contention based medium access relies on controlled connection between nodes to set up communication links. It does not require any infrastructure. Each node tries to access the channel independently based on the carrier sense mechanism [7]. But the problem with contention based MAC Protocol is collision probability increases with the increase in node density. Some important contention based MAC protocols are.

3.2.1 PAMAS (Power aware Multi-Access signaling)

PAMAS [8] is a contention based MAC protocol. It is designed with the main objective energy efficiency. It works on two different channels for data and control packets, which makes it more costly and complex in design. In this protocol node goes to sleep mode which are neither transmitting nor receiving the data.

3.2.2 S-MAC (Sensor MAC)

Sensor S-MAC [9] a contention based MAC protocol in which sensor node periodically goes to fixed listen/sleep duty cycle.

It reduces the energy consumption somehow, but has some drawback also. Fixed listen /sleep cycle increases the idle listening. Only in the listen period sensor node can communicate with other node and send some control packets like SYNC, RTS (Request to send), CTS (Clear to send), and ACK (Acknowledge). Here Figure-2 shows that node-1 wants to send data to node2.for that it firstly exchange control packets to all the neighbouring nodes. And then send data to specific node, in the meantime other neighbour nodes goes to sleep mode.

Node-1	SYNC	RTS	CTS RECV	DATA	ACK Recv
Node-2	SYNCRecv	RTSRecv	CTS	DATARecv	ACK
Node-3	SYNCRecv	RTSRecv	CTS	← SLEEP	

Fig.-2 Working of S-MAC protocol

Still a lot of energy is wasted due unnecessarily exchange control messages and idle listening to all the neighboring nodes. Many protocols have been proposed to improve the energy inefficiency of S-MAC protocol such as T-MAC (Timeout MAC) [10], Optimized MAC [11]. Optimized MAC gives better performance in terms of energy efficiency in which duty cycle varies according to the traffic on the network, and the network load is identified by the number of messages in a queue pending at a particular node.

3.2.3 B-MAC (Berkley-MAC)

B-MAC is advancement of S-MAC. In this protocol overhead of sending 4 control messages before sending every data packet is reduced by sending a preamble [12]. B-MAC is a good protocol for low traffic network. But if traffic on the network increases, sending preamble before every message transmission is a overhead. And thus preamble may be involved in a collision that may cause energy wastage. CCA mechanism in B-MAC is used to reduce the interference and noise from the medium. It is more energy efficient for the duration of no traffic. The preamble sampling technique may be more costly than sleep\active schedule protocol for high traffic networks. Another protocol is CC-MAC which is based on removal of spatial correlation [13]. Removal of spatial correlation will reduce the overhead of sending the same data by many sensor nodes. DSMAC is another Schedule based protocol which works on packet loss due to long queues and congestion control. The main motive of the DSMAC protocol is to minimize the medium Access delay that may occur due to high traffic rate.

3.2.4 STEM (Sparse topology and energy management)

A problem with basic preamble sampling technique is node has to mind the whole preamble even if he fires up-up in the center, or at the starting of preamble. Stem requires two radio channels. A separate channel for wakeup packet. In this protocol, instead of sending long preamble, a node sends a small wakeup packet. Receipentnt node of wakeup packet listens and replied with the small wakeup packet. After packet exchange transmitter will start sending data. If we denote the preamble length Tp, using the basic preamble sampling mechanism a transmitter node will take Tp time before sending every data packet. Wake up a time in STEM reduces this time to Tp/2.

3.2.5 Wise MAC

Wise MAC [14] solves the problem of energy wastage due to unnecessary sending the preamble and loosing energy wile every de ha affixed wakeup schedule. This scheme schedules the start of preamble packet, and save energy, by having a wakeup schedule of all the neighboring nodes. Another protocol, which is a combination of STEM and WiseMAC is introduced which is named a CSMA-MPS. And is reduces the energy consumption from both ends.

3.3 Schedule Based MAC Protocol

Protocol arbitrates modem access by finding a schedule to transmit, receive or active inactive. In a schedule based model of MAC protocols, energy wastage due to collision is reduced up to a certain level, but the disadvantage of schedule based protocol is the latency that occurred due to the synchronization of schedule. Much of the schedule based protocol uses local schedule synchronization which incurs the increase in delay of sending a frame. Some important schedule based protocol will be discussed ere and will be compared with their category of protocols on different parameters.

3.3.1 TRAMA (Traffic-Adaptive MAC protocol)

Is a schedule based energy efficient collision free protocol. It is based on time slot structure and uses distributed election scheme. The pairwise communication between neighbors is performed to schedule transmission slots. TRAMA consists of four main phases. Neighborhood discovery through NP (neighborhood protocol), Traffic information exchange through SEP and AEA (Schedule exchange protocol and adaptive election algorithms), and data transmission.

TRAMA increases the energy efficiency by increasing the time spent in the sleep mode. In addition TRAMA decreases the collision rate. However significant amount of end to end delay is occurred. Frame length is directly proportional to end to end delay, so by optimizing frame size end to end delay can be reduced. Still collision is possible, since TRAMA uses only information on one hop neighbors, hidden terminal problem can cause collisions in the network.

3.3.2 PAMAS (Pattern Based MAC)

Pattern based MAC is enhancement of TRAMA, a schedule based protocol. In this protocol schedule is determined on the basis of global information exchange. The collision probability of data is zero in this protocol that increases the energy efficiency in the low traffic network.

Still collision of schedule reservation message packets is possible, and exchange of global messages for schedule reservation will incur heavy traffic the network.

Another kind of reservation based protocol that is classified under the TDMA based protocol which uses TDMA as the schedule reservation method.

3.3.3 Energy Aware TDMA based MAC protocol

Energy aware TDMA based MAC protocol [19] is based on the formation of clusters and gateways. In this protocol, cluster head is elected based on the power level and range of the node. Gateway performs all the tasks. Gateway collects the data and send to another node within the cluster. Gateway is also responsible for slot assignment. The protocol operates in four phases IE data transfer, refresh, event based rerouting, and refresh based rerouting. For the slot assignment two techniques breadth first and depth first is used. Energy consumption in Energy Aware TDMA based protocol is reduced up to a certain level, but the problem arises due to clustering mechanism latency is increased and hence throughput of the network decreases. **BMA MAC** [16] is the advancement of this protocol. Which works in two phases 1st is a cluster setup phase and 2nd steady state phase. In cluster setup phase cluster head (CH) is selected based upon available energy of nodes. Steady state phase is used in each cluster. In which data period is split into two parts that is a data transmission period (fixed duration) and idle period. Slots are assigned here on demand. Whenever a node has to send data it will make a request to the CH by 1bit message. And after assignment of slot to the node, it will send the data in its own slot. We have categorized another kind of MAC protocol that is secure MAC protocol. In this category many protocols have been proposed so far. Our focus is to handle the node cloning attack. Here we will compare the protocol which is only related to node capturing attack.

3.4 Secure MAC protocol

For many sensor networks, security is a big issue like military applications of WSN need high level of security, in which the biggest IE is node capturing attack. Nodes are deployed in hostile environment, so if a node is captured, by using the information contained in that node, all types attack possible in WSN are now becoming easier for an attacker, and is called node cloning attack. One of the protocols that take care about the node capturing is LEAP.

3.4.1 Localized Encryption and Authentication protocol

In this protocol each sensor uses four different keys [18]. Individual key is a shared key between base station and sensor. Group key is shared between all the sensor and base station. Pairwise key is shared between two sensors. Cluster key is shared between neighbors of the sensor. Leap protocol uses a multi-broadcast authentication protocol like μ**TESLA.** It has loose synchronization and delayed authentication problem. LEAP is used to defend against node capture attack as well as it is protects from the intrusion in the network.

4. Comparison Table-1. Comparison of energy efficient MAC protocols

S. no	Protocols	classification	Collision	overhearing	Idle listening	Latency	Scalability	Node life-time	Network throughput
1	CSMA	Traditional Mac protocol	High	High	High	High	Not scalable for WSN	Less	Very Low
2	PAMAS	Contention Based	High	Low	Low	High	Very low	>CSMA	Low >CSMA
3	S-MAC(Sensor Mac or Sleep MAC)	Contention Based	High	Low<PAMAS	Low	LOW	Very low	>PAMAS	Low
4	Optimized MAC	Contention Based	High	Very Low<<S-MAC	Very Less<<s-MAC	LOW	For latency is not a concern	>S-MAC	LOW
5	B-MAC (Berkley MAC)	Contention based	High	Very Low	Low	Yes(Low)	Scalable for WSN with Low traffic	good	good

6	CC MAC(correlation based collaborative MAC)	Contention Based	High	LOW	Low	Very low	Less for dense WSN	Good	good
7	STEM(Sparse topology and energy management)	Contention Based	High	Yes(Low)	Low	Low	High	Low	Good
8	Wise MAC	Contention Based	Very Low	Very Low	Yes(Less)	YES(Low)	High	High	good
9	CSMA-MPS	Contention Based	Very Low	Overhearing of preamble is reduced	Yes (Less)	Low	high)	High	Good
10	TRAMA	Schedule Based	Yes (Very Low)	Very Less	Very Less	High	High for low traffic WSN	High	High
11	PAMAC(Pattern Based MAC)	Schedule Based	Ultra Low	Very Less	Very Less	High	Worse for heavily loaded WSN	High	High
12	Energy aware TDMA based MAC protocol	TDMA based	Ultra Low	Very Less	Less	High	Low		Less
13	BMA MAC	TDMA based	Collision free inside cluster	Low	Less	High	Low	High	Low

This protocol defends WSN against node capturing attack and also thwarts intrusion in the WSN. Problem with LEAP is energy consumption will increase with increase the number of nodes in the network. Also in this protocol node has to handle large number of keys the number of nodes in the network will increase.

3.4.2 Tiny Sec

Tiny Sec is a link layer, lightweight, generic security package that a WSN developer can easily introduce in their application. TinySec provides access control, message integrity and confidentiality for WSN. Tinysec uses a secure secret encryption key for all the WSN nodes.

Tinysec has two operating modes Tinyse AE (Authenticated encryption) and Tinysec A (Authentication only). TinySec has low energy consumption and lower memory space needed.

4. COMPARATIVE ANALYSIS

Comparative analysis of energy efficient MAC protocols is given by the Table -1 in which comparison is done on the basis of various parameters like collision, latency, scalability, network throughput, etc.

5. ENERGY EFFICIENT MAC PROTOCOLS

Energy efficiency is the main parameter of WSN MAC protocol due to limited battery capacity of WSN nodes, and difficulty in replacement of battery in every sensor nodes.

5.1 Contention based vs. Schedule Based. Contention based protocols like S-MAC, optimized MAC, B-MAC, Wise MAC are low latency protocol in which collision is possible. So based on the number of nodes in the network, the performance of network increases and decreases. While the schedule based protocol has a very less probability of collision, but have a significant latency problem. So schedule based protocols are well suited for applications that are not much concern about the little bit delay or latency. A contention based protocols are good for the applications which are more concern about end to end delay, however energy consumption due to collision are possible in every contention based protocol, but idle listening and other overhead are further reduced in the contention based advance protocol like Wise MAC.

6. SECURE MAC PROTOCOLS

6.1 LEAP vs. Tiny Sec. In secure MAC protocol we have discussed two protocols, LEAP and TinySec these protocols are used to provide security to attacks like node capture (node cloning) attack, intrusion, DOS jamming ets. LEAP is too heavy for WSN in comparison to Tinysec because it has to store the number of keys in a single node that consumes a lot of memory as well as not as much energy efficient. While Tinysec is a very lightweight link layer protocol. But it is not as much secure. TinySec consumes less energy, less bandwidth, but has not acceptable performed.

7. CONCLUSION

WSN is drawing much attention of researchers from the last ten years because of their real life useful application in almost every field. In this paper we have focused mainly on energy efficient WSN MAC protocols and some of the secure MAC protocols that provide protection against intrusion, node capturing, and replay attacks. Basically energy efficient WSN MAC protocols play a critical role in overall energy consumption in WSN. This paper gives the better comparative analysis of energy efficient MAC protocols, which further help in selecting desired protocol for the particular application.

REFERENCES

[1] Pei Huang, Li Xiao," The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey", *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013*

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,*” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, 2002".*

[3] I. Demirkol, C. Ersoy, and F. Alagoz, “MAC protocols for wireless Sensor networks: a survey,” *IEEE Commun. Mag., vol. 44, no. 4, pp. 115–121, 2006*

[4] Rajesh Yadav, Shirshu Varma, N. Malaviya "A SURVEY OF MAC PROTOCOLS FOR WIRELESS SENSOR NETWORKS*"UbiCC Journal, Volume 4, Number 3, August 2009*

[5] Eleazar Chukwuka1 and Kamran Arshad2 "ENERGY EFFICIENT MAC PROTOCOLS FOR WIRELESS SENSOR NETWORK: A SURVEY

[6] Simarpreet Kaur1* and Leena Mahajan2 "Power Saving MAC Protocols for WSNs and Optimization of S-MAC Protocol"*International Journal of Radio Frequency Identification and Wireless Sensor Networks, 02 June 2011*

[7] Akyildiz, Ian Fuat and mehmat can vuman."Wireless sensor networks"

[8] S. Singh and C. Raghavendra: PAMAS: Power Aware Multi-Access Protocol with Signalling for Ad-hoc Network, *ACM SIGCOMM Computer Communication Review (July 1998).*

[9] Wei Ye, J.Heidemann and D. Estrin: An Energy-Efficient MAC Protocol for Wireless Sensor Networks, *IEEE INFOCOM, New York, Vol. 2, pp. 1567-1576 (June 2002).*

[10] Tijs van Dam, Koen Langendoen: An Adaptive Energy Efficient MAC Protocol for Wireless Networks, in Proceedings of the *First ACMConference on Embedded Networked Sensor Systems (November 2003).*

[11] Rajesh Yadav, Shirshu Varma and N.Malaviya: Optimized Medium Access Control for Wireless Sensor Network, IJCSNS *International Journal of Computer Science and Network Security,Vol. 8, No.2, pp. 334 -338 (February 2008).*

[12] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. *In Proceedings of SenSys’04, pp. 95–107, Baltimore, MD, USA, 2004.*

[13] C. Schurgers, V. Tsiatsis, and M. B. Srivastava. STEM: topology management for energy efficient sensor networks. *In Proceedings of the IEEE Aerospace Conference, volume 3, pp. 1099–1108, Big Sky, MT, USA, 2002.*

[14] A. El-Hoiydi and J.-D. Decotignie. WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. *In Proceedings of the International Symposium on Computers and Communications (ISCC’04), volume 1, pp. 244–251, Alexandria, Egypt, July 2004.*

[15] K. Arisha, M. Youssef and M. Younis: Energy Aware TDMA based MAC for Sensor Network, in *IEEE Workshop on Integrated Management of Power Aware Communications Computing and Networking (IMPACCT’02) (2002).*

[16] J. Li and G. Y. Lazarou. A bit-map-assisted energy-efficient MAC scheme for wireless sensor networks. In *Proceedings of ACM IPSN’04, pp. 55–60, Berkeley, CA, USA, April 2004*

[17] S. Mishra and A. Nasipuri. An adaptive low power reservation based MAC protocol for wireless sensor networks. In *Proceedings of the IEEE International Conference on Performance, Computing, and Communications, pp. 731–736, Phoenix, AZ, USA, April 2004.*

[18] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN), vol. 2, pp. 500-528, 2006.*

[19] K. A. Arisha, M. A. Youssef, and M. Y. Younis. Energy-aware TDMA-based MAC for sensor networks. *Computer Networks, 43(5):539–694, December 2003.*