*Gazi University Journal of Science*
*GU J Sci*
*25(2):455-464 (2012)*

**ORIGINAL ARTICLE**

GUJS

# Medium Access Control Protocols For Wireless Sensor Networks: Literature Survey

Murat DENER [1‡], Ömer Faruk BAY [1]

[1] *Gazi University, Faculty Of Technical Education, Department of Electronic-Computer Education, Ankara, Turkey*

*Received:* 21/04/2010 *Revised*:07/07/2010 Accepted: 04/02/2012

**ABSTRACT**

Wireless Sensor Networks (WSNs) have become an active research area for the researchers. Although sensor nodes have low processor, low memory and limited energy, they have capabilities with random located, self organizing, collective work, and local computation. WSNs consist of these nodes. WSNs are feasible in military, healthcare, environmental, home automotion and commercial applications. Various Medium Access Control (MAC) protocols with different objectives were proposed for WSNs. In this paper, we first outline the sensor network properties that are crucial for the design of MAC layer protocols. Then, we describe several MAC protocols proposed for sensor networks emphasizing their strengths and weaknesses. Also, we have presented security problems and solutions on MAC protocol. Finally, we point out open research issues of MAC layer design. It is considered that this study will help to MAC protocol designers.

**Keywords:** Medium Access Control Protocol, Wireless Sensor Networks, Energy Efficiency, Wireless Network Security, Attributes of MAC Protocol

## 1. INTRODUCTION

Developments in low - cost sensor architecture made Wireless Sensor Networks (WSNs) a new and popular research area. These networks occur when a great number of low-power and low-cost sensors which have limited capacity and short-range transmitter are randomly left in a medium that is not easily accessible and most of the time is unreliable. Each node has computing, sensing and communication capabilities. These nodes which can be randomly distributed to the observed medium can recognize each other and realize the measurement in a wide area together. Thanks to these properties, they can be used in various areas from healthcare to military and from building safety to early detection of forest fires [1-4].

Today, there are improvements in software and hardware in order to make sensor networks more practical. However, reducing energy consumption per unit and thus increasing the lifespan of the sensor nodes lies in the basis of any work being done. The main reason why lifespan is so important is that replacing or re-filling the sensors in the work environment and energy resources are most of the time impossible and too costly [5]. Moreover, energy consumption of the nodes affects the life-span of WSNs. For this reason, effective energy use of the nodes is of great importance to WSNs. In addition to reducing energy consumption in sensor networks unnecessary use of energy should be reduced. Many studies are being done to find more effective and efficient energy use in academic circles and industries. These studies are further concentrated on the data link layer and the network layer. While studies on network layer are concentrated on data routing, studies on data link layer are mostly concentrated on MAC protocols, which are concerned with wireless environment access methods.

MAC protocols have a significant effect on the function of WSN. MAC protocol, which builds bottom infrastructure in sensor network systems, decides how to use wireless channel and allocate limited wireless communication resources for sensor nodes. MAC protocol, one of the key network protocols that ensure effective communication in sensor network, is in the bottom part of the sensor network protocol and has a great impact on the performance of sensor network [6].

‡Corresponding author, e-mail: muratdener@gazi.edu.tr

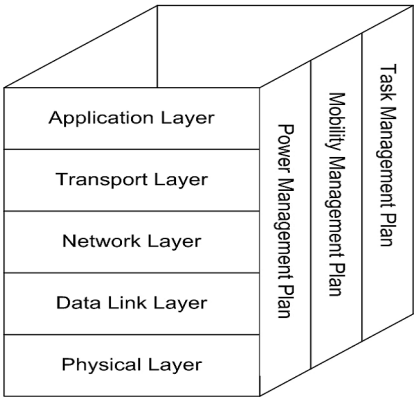


Figure 1. Architecture of a WSN communication protocol

The Data Link Layer must provide timely and reliable peer-to peer communications, namely a MAC mechanism for managing distributed access to a shared transmission medium with minimum power consumption and communication overhead. The Data Link Layer (DLL) is mainly divided into 2 sublayers: Logical Link Control (LLC) and Medium Access Control (MAC). A common challenge of the DLL is to schedule the available data for transmission (in the overall network) and provide a mechanism for each node to decide when and how to access the shared medium to transmit its data. These functionalities are basically performed by Medium Access Control (MAC) protocols [7].

Because there no any standard in WSNs in terms of MAC protocol, a great number of studies about MAC are being done in literature. While developing approaches to minimize energy consumption is the primary aim in most of these studies, latency is the second issue. However, it is necessary to use security protocols that enable secret data transfer from sensors to the base station during critical WSNs applications such as spying enemy lines or border regions. However, low processor and radio capacities of sensors do not allow the application traditional security protocols to WSNs [2]. Therefore, MAC - layer security issues and solutions are presented in this article.

A research related to MAC protocols in WSNs is done in this study. Attributes of a good MAC protocol, main sources of energy consumption, MAC-layer security issues and solutions are described in Section 2. Strengths and weaknesses of many proposed MAC protocols are presented in Section 3. A comparison of different MAC protocols is made in Section 4. Open research topics in this field are given in Section 4 and the results of the study are emphasized in Section 5.

## 2. MAC PROTOCOL DESIGN CHALLENGES

It is necessary to establish communication links between nodes because a great number of sensor nodes are distributed to the medium in Wireless Sensor Networks. For this reason, MAC protocol has two aims in WSNs. The first is to build a sensor network infrastructure. The second is to share the communication medium in a fair and efficient way. [8]

### 2.1. Attributes of a Good MAC Protocol

Attributes that should be taken into consideration in the design of MAC protocol are listed on Table 1 [9-11].

Table 1. Attributes of a Good MAC Protocol

| | |
|---|---|
| *Energy efficiency* | Energy efficiency is the most important issue when designing a new MAC protocol in WSNs because the networkôs lifetime is determined by the nodesô energy. |
| *Latency* | The elapsed time for sending a MAC-layer data packet successfully is called ñLatencyò. |
| *Throughput* | The ratio of the messages served by communication systems is called ñThroughputò. |
| *Robustness* | Robustness is composed of the attributes including reliability, usability, and durability. It shows the protocolôs degree of resistance to errors and false information. |
| *Scalability* | Capability of communication system regardless of the number of sensor nodes performing a transaction and the size of the network is called ñScalabilityò. |
| *Stability* | The ability of communication system to handle the issue of traffic congestion in the medium that changes constantly is called ñStabilityò. A stable MAC protocol should handle sudden loads that can exceed maximum channel capacity. |
| *Fairness* | Bandwidth is limited in most of WSNs applications, but the base station must receive data equally from all the nodes. Channel capacity should be fairly shared among the nodes without reducing the efficiency of the network. |

### 2.2. Major Sources of Energy Consumption

MAC protocol makes it possible to share communication resources that have a common MAC protocol among the nodes in an efficient and fair way. MAC protocol carries with it a set of rules that determines which node is allowed access to the medium. Most of the power is consumed by a radio in a node. So, MAC is greatly important in terms of power management. Energy in WSNs is mainly consumed in four simple ways [9,12].

- *Collision:* When there is a collision, the packet has to be omitted and re-sent. This event both increases energy consumption and leads to latency.

- *Overhearing:* This occurs when a node receives a packet that is directed to other nodes.

- *Control Packet Overhead:* Control packets that are used for sending and receiving consume a lot of energy.

- *Idle listening:* This represents the standby state during which a packet is received, although there is no packet sent in the network. If a node does not transmit or receive, if it has no packet, or if it can not send the packet because its neighboring node is in transmission even though it has a packet, it is said that this node is listening to the medium unnecessarily.

Energy consumption should be minimized in a designed MAC protocol by preventing the reasons identified above.

### 2.3. MAC and Security

Sensor nodes in WSNs should obey some security rules while communicating with one another and sending detected data to the base station [13, 14]. There are some security requirements on WSNs. They are listed in below.

**Data Condentiality** of data means to assure that information contained in the data is only disclosed to users or devices for which the data was intended. **DataAuthentication** of data means to assure that a receiver of the data is able to check whether the data originates from the claimed sender or not. **Data Integrity** ensures that the data which receiver receives has not been tampered or replaced by the attacker during the trasmission. **Data Freshness** refers that the data is the latest data in the recent time, which is passed from senders to receivers.

Another security requirement is data availability. It ensures that services and information can be accessed at the time that they are required. There are many risks that could result in loss of availability such as sensor node capturing and DOS attacks. Researchs [15] investigated the issue of DOS in 802.11 wireless networks. Also, they proposed a security model to be used in prospective IEEE 802.11 standards for countering DOS attacks.

In addition, vulnerabilities and solution of MAC protocols methods are given in the following paragraphs [16]. These issues should be taken into consideration for those applications requiring security such as military and medical applications.

- *Continuous Channel Access (Exhaustion):* A malicious node disturbs the MAC protocol with continuous requests for sending and receiving over the channel. As a result, other nodes can not access the channel. In the event of such an attack, excessive demands can be ignored by checking MAC management thereby preventing lose of energy due to repeated mappings. A second technique is to use time-division multiplexing that separates one time zone when mapping to each node [17, 18].

- *Collision:* This is similar to constant channel attack. Collision occurs as a result of the simultaneous attempts of two nodes to send at the same frequency. When packets work, data division will probably occur and there will be unmapped data at the end of receiving. Then, the packet will be invalid and it will be omitted. Packet collisions can be prevented by using error-control codes [17, 18].

- *Unfairness:* Repetition of MAC layer attacks, such as consumption and collision or abuse of the priority mechanism that belongs to the MAC layer, lead to unfairness. These kinds of attacks are partly known as DOS attacks. Small-sized frames can be used as a defense method against these attacks. In addition to this, unfairness can be prevented by using each separate node channel for a short period [17, 18].

- *Interrogation:* Hidden terminal problems of MAC protocol can be largely reduced with the help of handshake of request-to-send, RTS and clear-to-send, and CTS. An attacker can consume sources of a node by constantly sending RTS messages and receiving CTS messages. Attacks can be prevented to requests from the same node or Anti-replay and strong link layer architecture [19, 20].

- *Sybil Attack:* At a Sybil attack involves a malicious sensor node introducing itself to the other nodes in the network with multiple identities. In this case, the messages from that malicious node are perceived as coming from different nodes by the victim node. The malicious node can hinder the victim node from receiving and sending messages. Moreover, a malicious node can greatly change the information gathered in the network by constantly sending false information through a Sybil attack. Thus, it can mislead the decision-making mechanism by causing the base-station to gather false information. Radio resource testing and random key distribution methods are used in order to prevent this attack [20, 21].

## 3. PROPOSED MAC PROTOCOLS

MAC protocols for Wireless Sensor Networks are classified into 2 categories: contention based (CSMA ï based) and TDMA - based. In TDMA ï based protocols, packet collision, unintentional receiving and unnecessary listening to the medium can be avoided by utilizing sending and listening periods, but a strict synchronization is needed. On the other hand, in the contention based protocols, synchronization is flexible

and the addition of new nodes can be easily adjusted to topology changes such as replacing exhausted nodes in the network and adding new nodes to the network after a few years. CSMA-based protocols have higher costs in the case of packet collision, unintentional receiving and unnecessarily listening to the medium [8, 22]. Table 2 shows comparison of TDMA and CSMA.

Table 2. Comparision of TDMA and CSMA

| TDMA | CSMA |
|---|---|
| Strict Synchronization | Synchronization is flexible |
| Controlled Access | Random Access |
| High Channel Utilization under high contentions | High Channel Utilization under low contentions |
| Need Central Control | Completely decentralized |

MAC protocols in WSNs are generally CSMA-based. CSMA is popular because it is simple, flexible and durable. It does not need much infrastructure support. It does not require clock synchronization and global topology knowledge. When a node joins or leaves the network dynamically it can be controlled without an extra operation. After all, a node can receive a packet from two different nodes which are not in the same coverage area. Packet collision occurs thusly. This problem is known in literature as a hidden terminal problem. This problem leads to energy loss in sensor applications. Fortunately, hidden terminal problems can be alleviated by using a RTS/CTS operation. However, additional load comes to the network due to RTS/CTS messages because data packets are small in the sensor networks.

On the other hand, TDMA provides a solution to the hidden terminal problem without a need for extra messages because it programs the transmission time of neighbor nodes at different times. However, TDMA also has some disadvantages. First of all, there should be an effective timing program in order to avoid packet collision. However, an efficient timing program is very difficult with a high degree of compatibility and reuse of the channel. Secondly, TDMA requires strict clock synchronization, a necessary feature for most sensor applications that leads to a high energy load. Thirdly, topology in sensor networks often changes due to reasons such as the conditions of the physical environment, battery cuts, or corruption of the node. It is quite costly for TDMA to control dynamic topology changes. Fourthly, it is difficult to detect the mixed relationships between neighbor nodes because radio mixture range is different from communication range. Moreover, some mixture nodes may not be directly within the communication range. Finally, TDMA allows low channel use during low latency and leads to a higher latency when compared to CSMA because a node in TDMA can only transmit in its own time zone. As for CSMA, nodes can always transmit unless there is a collision.

Traditional MAC protocols can not be used directly in WSNs because of structural differences. While quality of service is the primary goal in traditional MAC protocols, the priority in WSNs is to reduce power consumption [23]. Therefore, various MAC protocols with different goals were developed for WSNs. Table 3 shows a comparison of investigated MAC protocols.

Table 3. Comparision of MAC protocols

| **Mac Protocols** | **Priority** | **Type** | **Simulation environment** |
|---|---|---|---|
| IEEE 802.11 | Energy | CSMA | TinyOS (micaz, telosb) |
| IEEE 802.15.4 | Energy | CSMA | TinyOS (micaz, telosb) |
| S-MAC | Energy | CSMA | TinyOS (micaz) + ns2 |
| T-MAC | Energy | CSMA | OMNeT++ |
| DSMAC | Latency | CSMA | ns2 |
| P-MAC | Energy | CSMA | ns2 |
| PAMAS | Energy | CSMA | Developed by author |
| Optimized MAC | Latency | CSMA | ns2 |
| TRAMA | Energy | TDMA | Qualnet |
| ALOHA with Preamble Sampling | Energy | ALOHA | Developed by author |
| WiseMAC | Energy | CSMA | ns2 |
| B-MAC | Energy | CSMA | TinyOS (micaz) |
| X-MAC | Energy | | MOS (telosb) |
| Z-MAC | Energy | CSMA + TDMA | TinyOS (micaz) + ns2 |
| MH-TRACE | Energy | TDMA | ns2 |
| TRACE | Energy | TDMA | ns2 |

IEEE 802.11 [24] is a CSMA-based MAC protocol that uses a random withdrawal method and carrier signal listening in order to prevent data packet collision in WSNs. A node that wants to send a message to the IEEE 802.11 protocol listens to the medium for a short period and then starts to send the message if the channel is empty; the IEEE 802.11 protocol verifies the channel is empty if it does not perceive any communication from the nodes. Nodes in 802.11 have to contend with the other nodes in order to get the right to transmit to

the MAC. The node that loses the contention must wait and try again. Power Save Mode (PSM) in this protocol prevents unnecessary listening to the medium by periodically passing to a dormant state.

IEE 802.15.4 [25, 26], a CSMA/CA ï based protocol determines MAC and Physical Layers for Wireless Private Area Networks (WPANs). Although this protocol is not specifically developed for WSNs, it can be used for WNSs because of its low power consumption, low-cost and flexibility. Presently, this protocol works on the Micaz and Telos nodes produced by Crossbow [27].

S-MAC [9] is a CSMA ï based MAC protocol designed with a modified IEEE 802.11. Its primary goal is power consumption. The innovations in this protocol are periodical listening, reducing collision, preventing unintentional receiving, and message transition. Nodes generally sleep instead of continuously listening to the medium. Listening and sleeping times are stable and periodic. There should be a strict synchronization so that the nodes can move together. The timing diagram of S-MAC is shown in Figure 2.

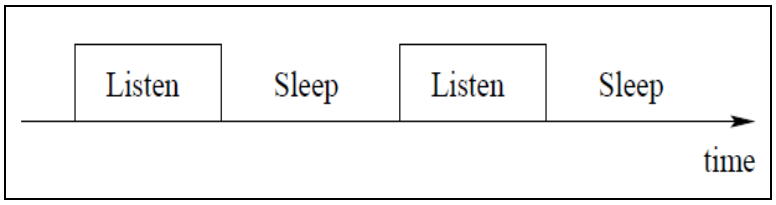


Figure 2. S-MAC

S-MAC supports message transition so that large-sized packets can be sent more efficiently. The positive aspect of S-MAC is that there is a TinyOS [28] operation system version written in the language of nesC [29] running on the simulation model and sensors; this reduces energy consumption significantly. The negative aspect of S-MAC is that the nodes need a strict synchronization in order to move together; due to stable listening/sleeping timing it does not synchronize and thus latency increases.

T-MAC [30] is a CSMA-based MAC protocol developed for WSNs. Although stable sleeping-listening periods in S-MAC increase energy efficiency, they also lead to high latency and low-efficiency. T-MAC is proposed to improve weak results of S-MAC during variable traffic densities. If any communication does not occur during a certain period of listening time in T-MAC (timeout, TA), sleeping mode occurs. This situation is shown in Figure 3.

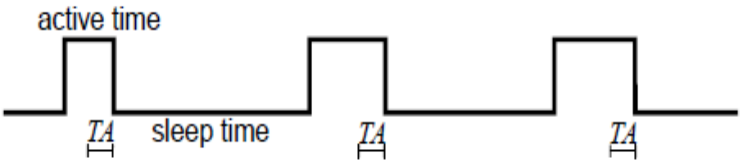


Figure 3. T-MAC

T-MAC consumes less energy than S-MAC, but causes more latency.

P-MAC [31] is a CSMA ï based MAC protocol developed for WSNs. Most of the MAC protocols like S-MAC sleep periodically to save energy. Duty cycle is constant in these protocols. Instead of stable sleeping and listening periods, sleeping-listening periods in P-MAC are determined in a different way. Timing is determined by the traffic of the node and its neighbors. Figure 4 shows S-MAC, T-MAC and P-MAC periods in the event that there is no traffic.

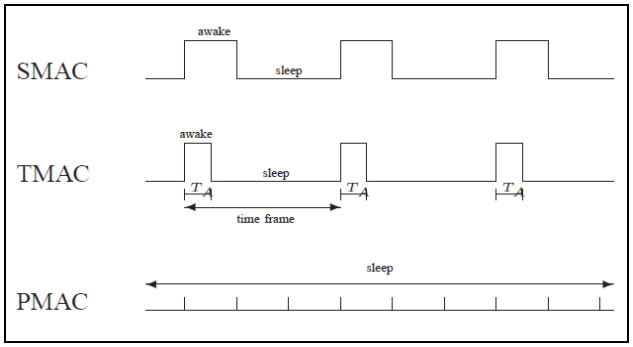


Figure 4. P-MAC

DSMAC [32] has added a dynamic time zone feature to the S-MAC protocol. Its goal is to reduce latency for delay-sensitive applications. All the nodes share one hop latency in SYNC period (the elapsed time between the meeting packet in the queue and sending it) and also start in the same time zone. Figure 5 shows the DSMAC dynamic time cycle.

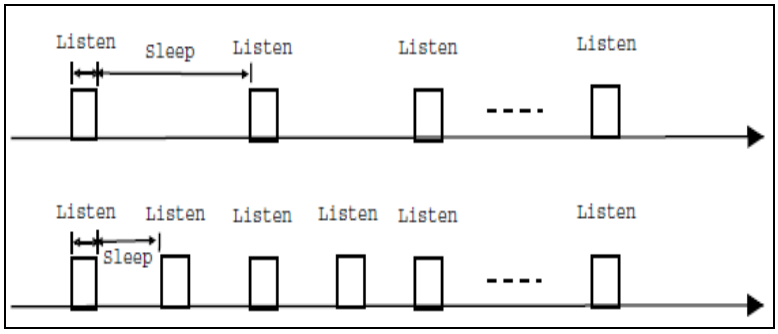


Figure 5. DSMAC

PAMAS [33] is a CSMA based multiple access protocol in which the main goal is energy efficiency. This protocol was generated by adding separate signal channels to the MACA [34] protocol. PAMAS uses two separate channels for data and control packets. It needs two radios in different frequency bands. The feature that distinguishes this protocol from MACA is the fact that the radio of the nodes that are neither transmitting nor receiving are closed in order to save energy. There is a significant power loss in PAMAS because significant switching is done in the cases of sleeping and listening. Closing the nodes does not cause latency in PAMAS because the node is only closed when unnecessarily listening to the medium. Unintentional receiving, which occurs when a node receives the packets routed to other nodes, is hindered in PAMAS. PAMAS needs two independent radio channels, which results in two independent radio systems in every sensor node.

The nodesô duty cycle can change according to network load in the Optimized MAC [35] protocol. If there is heavy traffic the duty cycle will be high but if there is low traffic the duty cycle will be small. Network load is defined as the number of messages in the queue. Additional loads that control packetsô causes are less when compared to S-MAC protocol because the size and number of the control packets are reduced in Optimized MAC. This protocol can be used in healthcare and defense applications requiring low latency and energy efficiency.

TRAMA [36] is a TDMA-based MAC protocol designed for energy efficiency. Energy consumption is reduced in this protocol by switching off when nodes are neither transmitting nor receiving, that is, when they are free and therefore guaranteeing that a packet collision will not occur. TRAMA consists of three main components. First, the neighbor protocol (NP) gathers information from neighbor nodes. Schedule Exchange Protocol (SEP) allows nodes to exchange two-hop neighbor information and programs. Adaptive Election Algorithm (AEA) decides on the nodes that will transmit and receive in the current time zone by using neighbor and program information. This protocol is used for energy efficiency and applications requiring efficiency apart from the delay-sensitive applications. TRAMA provides higher efficiency and more energy than S-MAC. TRAMA leads to more latency when compared to CSMA-based protocols such as IEEE 802.11 and S-MAC.

Aloha with preamble sampling [37] is a MAC protocol that combines ALOHO [38] protocol with preamble sampling, which is one of the energy conservation techniques. The main disadvantage of ALOHO protocol is the energy loss due to unnecessarily listening to the medium. El-Hoiydi [33] proposes low-power listening technique to prevent this situation. This approach works in the Physical Layer. The heading starts with the preamble indicating the receiver of the incoming messages. The receiver opens the radio channel periodically in order to sample incoming message when

the preamble is noticed and continues to listen for normal message transfer. If the preamble is not noticed, the radio station closes until the next sample. This protocol is suitable for applications requiring low traffic.

WiseMAC [39] is a MAC protocol developed for WSNs. WiseMAC is similar to TDMA in Space that all the sensor nodes use two communication channels and CSMA protocol in Preamble Sampling. While TDMA is used for access to a data channel, CSMA is used for access to a control channel. After all, WiseMAC only needs one channel and uses non-persistent CSMA and Preamble Sampling in order to reduce its power consumption during unnecessary listening to the medium. According to the simulation results, WiseMAC is more efficient than the S-MAC protocol.

B-MAC [40] is a CSMA-based MAC protocol designed for WSNs. It is similar to Aloha with a preamble sampling in that the sensor node is opened and closed repetitively without losing data packets in the receiver-sender duty cycle. After all, the size of the preamble is supplied as a parameter in the upper layer. This condition enables optimum exchange during energy conservation, latency, and efficiency. Moreover, another method of reducing energy is Clear Channel Assessment (CCA) [41]. A threshold is determined for signal strength in CCA. When a message is ready for transmission, signal strength and threshold are compared, this way the mixtures in the signal are identified. The goals of this protocol are: low power consumption, active collision avoidance, small code and memory usage, effective use of the channel in low and high data rate, resistance to changeable medium conditions and suitability for a large scale. B-MAC has a better performance in latency, efficiency and energy consumption when compared to S-MAC.

X-MAC [42] is inspired by B-MAC. It is one of the protocols that has low-power listening. The node remains awake to collect arriving data transmissions and listens to the medium in low-power listening. If no data arrives, it passes to the dormant state. Otherwise, the node waits for completion of packet transmissions. After ensuring that packet receiving is completed, preamble time is added. The low-power listening technique does not give equal right to the nodes. The low-power listening technique is simple, not synchronous, and provides energy efficiency. Long preamble increases latency and is inadequate in terms of energy consumption. X-MAC solves these problems with a short preamble approach in a method called low power communication without losing the advantages of the low-power listening technique. Low-power communication is simple and it parses receiver and sender sleeping programs. This approach in X-MAC reduces energy use in both receiver and sender. Moreover, latency is also reduced by using a short-preamble. During one-way transmission, it has better results in latency, efficiency and power consumption when compared to B-MAC. Energy loss due to unintentional listening is decreased. It is similar to B-MAC in broadcast transmissions.

Z-MAC [43] is a MAC protocol that combines the strengths of CSMA and TDMA. While it succeeds at low latency and high channel use during low contention, it succeeds high channel use during high contention in the same manner as TDMA. The differences from CSMA and TDMA can be listed as being resistant to synchronization errors, failure in selecting time zone and changing channel conditions. As a disadvantage, performance of Z-MAC is never as good as CSMA. Z-MAC is implemented on TinyOS. Although it is written on TinyOS, it is hard to apply it to the nodes. Even though none of the nodes are transmitting, nodes in Z-MAC can still be awake.

Multi-Hop Time Reservation Using Adaptive Control for Energy Efficiency (MH-TRACE)[44] is a distributed MAC protocol for energy efficient real-timepacket broadcasting in a multi-hop radio network. There are two techniques used in MH-TRACE to save energy. The first technique is to reduce energy dissipation at the MAC layer. The second technique is to reduce energy dissipation using an application dependent cross layer approach, namely, avoiding packet receptions that will he discarded at the higher layers of the protocol stack if not avoided at the MAC layer. The most important advantage of MH-TRACE is that it achieves traffic adaptive energy efficiency in a multi-hop network without using any global information except synchronization.

Time reservation using adaptive control for energy efficiency (TRACE) [45] is a time frame based media access control (MAC) protocol designed primarily for energy-efficient reliable real time voice packet broadcasting in a peer-to-peer, single-hop infrastructureless radio network. TRACE is an energy-efficient dynamic time-division multiple-access (TDMA) protocol designed for real-time data broadcasting. TRACE has better energy saving and throughput performance than PRMA and IEEE 802.11.

The primary goal of the investigated protocols was energy efficiency which is important for WSNs. T-MAC and DSMAC protocols were developed by making some additions to S-MAC. As for X-MAC, it improved one-way transmission by shortening preamble used in B-MAC protocol. There is some researchs [46,47] that compare some MAC protocols (IEEE 802.11, CPS, MH-TRACE) in terms of packet delivery ratio, packet delay, delay jitter, energy dissipation and error resilience. According to researchs MH-TRACE has good results than others. The protocols running on TinyOS are more useful, because they can be used in real applications. The reason that the protocols are mostly CSMA-based is because TDMA can not keep up with dynamic topology changes. For this reason, it becomes difficult to provide the scalability principle, which is one of the important characteristics of WSNs.

## 4. RESULTS AND DISCUSSIONS

We need to have set of protocols to perform successful transmission among different nodes. With these protocols channel acquisition and synchronization among nodes becomes better and success of transmission increases. MAC layer is mainly responsible for doing the above functions. There are more steps for design a MAC protocol. First, researchers have to decide that in which application do they use this protocol. Because there are more priority such as energy efficiency, latency, throughput, security. If your first priority is energy efficiency, you can neglect to more security. Because, each work for security causes that energy consumption and delay. Otherwise, if you develop a protocol which will be use in military or healthcare applications, you have to provide security requirements. In order to meet the application level security requirements, the individual nodes must be capable of performing complex encrypting and authentication algorithms. Long mechanism of encryption and decryption should not be kept as they consume more energy. In WSNs, energy efficiency is the main task. There are large opportunities of energy savings at the MAC layer. Sensor nodes have to be designed to manage its local supply of energy in order to maximize total network lifetime. Also, response time is the time taken by any node to respond a query. This parameter is important during real traffic. Moreover, security is the main concern for any network. Wrong data passing or passing data to wrong person will always cause problem to the network.

After surveying the effect of the parameters like power, lifetime of sensor network, memory, security and type of radio communication on different protocols, it can be concluded that these evaluation parameters should be kept in mind while designing MAC protocol.

## 5. CONCLUSION

A great number of MAC protocols for WSNs have been proposed by researchers lately. However, none of these protocols have been accepted as a standard because MAC protocols are specific to each application. In this paper, several MAC protocols are described that proposed for sensor networks emphasizing their strengths and weaknesses. Security problems and solutions on MAC protocol are presented. Open research issues of MAC layer design is given. It is considered that this study will help to MAC protocol designers.

In recent years, a great number of MAC protocols for WSNs have been designed and published by researchers. The primary issue focused on, relating to MAC protocols, has been energy efficiency. After all, as it is indicated below, several studies can be done in different areas for MAC protocols.

- *Assessment on Sensor Platforms:* Most of the MAC protocols proposed for WSNs were assessed in a simulation environment. However, it is necessary to assess the performed MAC protocols on the wireless sensor nodes (micaz, telosb, iris, etc.) produced by Crossbow. Researchers should have experience on the real sensor platforms and then focus on their new studies.

- *Real-time systems:* Energy efficiency is the primary goal of MAC protocol design in sensor networks. However, security measures that enable secret data transfer from sensors to the base station should be considered in the critical WSNs applications, such as spying on enemy lines or border regions. Otherwise, an offensive node left in the medium can damage the network structure and send false information to the base station. Researchers should also work on security issues in real-time systems.

- *Flexibility:* MAC protocols in WSNs generally are specific to the application. For instance, security is the primary goal for military applications (target acquisition, keeping a battlefield under supervision, intrusion detection), low-latency is the primary goal for healthcare applications (monitoring patients at hospitals, keeping seniors under supervision), and energy efficiency is the primary goal for some applications (monitoring an ecological region). Any MAC protocol that is developed should provide all of these attributes such as energy efficiency, low-latency, high efficiency and security.

## ACKNOWLEDGMENT

Thanks are due to Scientific Research Project Foundation of Gazi University, Ankara, Turkey for providing a financial support (Project code no: 07/2010-04)

## REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., ñA survey on sensor networksò, ***IEEE Communications Magazine*** 40(8): 102-114, 2002.

[2] Ozdemir, S., ñSecure Data Aggregation In Wireless Sensor Networks Via Homomorphic Encryptionò, ***J. Fac. Eng. Arch. Gazi Univ***., 23(2): 365-373, 2008.

[3] Chong, C-Y., Kumar, S.P., ñSensor Networks : Evolution, opportunities, and challengesò, ***Proc IEEE,*** 91(8): 1247-1256 (2003).

[4] Cakiroglu, M., Ozcerit, A.T., ñDenial Of Service Attack Resistant Mac Protocol Design For Wireless Sensor Networksò, ***J. Fac. Eng. Arch. Gazi Univ***., 22(4): 697-707 (2007).

[5] R. Lin, Z. Wang, Y. Sun, ñEnergy Efficient Medium Access Control Protocols for Wireless Sensor Networks and Its State-of-Artò, ***IEEE,*** 669-674, (2004).

[6] D. Wen, C. Zhi-jiang, L. Xiu-mei, ñResearch progress on MAC protocol for wireless sensor networkò, ***IEEE***, (2011).

[7] A. Koubaa, M. Alves, E. Tovar, ñLower Protocol Layers for Wireless Sensor Networks: A Surveyò, ***IPP-HURRAY Technical Report***, HURRAY-TR-051101 (2005).

[8] Yadav R., Varma S., Malaviya N., ñA Survey Of Mac Protocols For Wireless Sensor Networksò, ***UbiCC Journal***, 4 (3) (2009).

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

[10] G.D. Bacco et al., ñA MAC Protocol for Delay-Bounded Applications in Wireless Sensor Networksò, ***Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop***, (2004).

[11] Sohraby K., Minoli D., Znati T., ñWireless Sensor Networks Technologyò, Protocols and Applications, ***A John Wiley & Sons***, A.B.D., (2007).

[12] Tijs van Dam, Koen Langendoen, ñAn Adaptive Energy Efficient MAC Protocol for Wireless Networksò, ***Proceedings of the First ACM Conference on Embedded Networked Sensor Systems,*** (2003).

[13] Karaboŋa D., Ökdem S., ñSecurity Communication Techniques on Wireless Sensor Networksò, ***Electronic Signature Semposium***, (2006).

[14] Perrig, A., Szewzyk, R., Tygar, J.D., Wen, V., and Culler, D.E., ñSPINS: security protocols for sensor Networksò, ***Wireless Networks***, 8, 521-534, (2000).

[15] K. Bicakci, B. Tavli, ñDenial of Service Attacks and Countermeasures in IEEE 802.11 Wireless Networksò, ***Computer Standards & Interfaces Journa***l, 31 :931-941 (2009).

[16] T.Kavitha1, D.Sridharan, ñSecurity Vulnerabilities In Wireless Sensor Networks: A Surveyò, ***Journal of Information Assurance and Security,*** 5: 031-044, (2010).

[17] Mohit Saxena, ñSecurity In Wireless Sensor Networks - A Layer Based Classificationò, ***Cerias Tech Report***, (2007).

[18] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, ñA Survey Of Security Issues In Wireless Sensor Networksò , ***IEEE Communications Surveys & Tutorials,*** 8:2, 2nd Quarter, (2006).

[19] Hiren Kumar Deva Sarma, Avijit Kar, ñSecurity Threats in Wireless Sensor Networksò, ***IEEE***, (2006).

[20] Raymond D.R. Midkiff.S.F, ñDenial of Service in Wireless Sensor Network: Attacks and Defensesò, ***IEEE Pervasive Computing***, 7(1): 74 ï 81, (2008).

[21] Meghdadi M., Ozdemir S., Güler Ķ, ñSecurity in Wireless Sensor Networks:Problems and Solutionsò, ***International Journal Of Information Technologies***, 1: 35-40, (2008).

[22] Demirkol Ķ, Ersoy C., Alagöz F., ñMac Protocols for Wireless Sensor Networks: a Surveyò, ***IEEE Communication Magazine***, 115-121, (2006).

[23] P. Le-Huy, S. Roy, ñLow-Power Wake-Up Radio for Wireless Sensor Networksò, ***Mobãle Networks & Applēcatēons,*** 15(2): 226-236 (2010).

[24] ñPart 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specificationsò, ***IEEE Standards*** 802.11, 195-200,(1999).

[25] IEEE-TG15.4, ñPart 15.4: Wireless Medium Access Control (MAC) anf Physical Layer (PHY) Specifications for Low-Rate Wireless Personel Area Networks (LR-WPANs)ò, ***IEEE standart for Information Technology***, (2003).

[26] A. Koubaa, M. Alves, E. Tovar, ñIEEE 802.15.4: a Federating Communication Protocol for Time-Sensitive Wireless Sensor Networksò, ***Sensor Networks and Configurations: Fundamentals, Tecniques, Platforms and Experiments,*** Springer-Verlag, Germany 19-49, (2007).

[27] Crossbow Technology Inc., http://www.xbow.com, 2010.

[28] Tiny-OS, http://www.tinyos.net/, 2010.

[29] D.Gay, P. Levis, R. Von Behren, M. Welsh, E. Brewer, D. Culler, ñThe nesC Language: A Holistic Approach to Networked Embedded Systemsò, ***Programming Language Design and Implementation,*** (2003).

[30] T.V. Dam and K. Langendoen, ñAn Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networksò, ***The First ACM Conference on Embedded Networked Sensor Systems (Sensysó03)***, Los Angeles, CA, USA, November, (2003).

[31] T. Zheng, S. Radhakrishnan, V. Sarangan, ñPMAC: An Adaptive energy-efficient MAC protocol for Wireless Sensor Networksò, IPDPS õ05: ***Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium***, (2005).

[32]. P. Lin, C. Qiao, and X. Wang, ñMedium access control with a dynamic duty cycle for sensor networksò, ***IEEE Wireless Communications and***

***Networking Conference***, 3 (1534 ï 1539): 21-25, (2004).

[33] S. Singh and C. Raghavendra: ñPAMAS: Power Aware Multi-Access Protocol with Signaling for Ad-hoc Network, ACM SIGCOMMò ***Computer Communication Review,*** (1998).

[34] P. Karn,"MACA -a New Channel Access Method for Packet Radio",***in ARRL/CRRL Amateur Radio 9tt,Computer Networking Conference***,134-140, (1990).

[35] Rajesh Yadav, Shirshu Varma and N.Malaviya: Optimized Medium Access Control for Wireless Sensor Network, ***IJCSNS International Journal of Computer Science and Network Security***, 8(2): 334-338, (2008).

[36] V. Rajendran, K. Obraczka and J.J. Gracia-Luna-Aceves: Energy Efficient, Collision Free Medium Access Control for Wireless Sensor Networks, in ACM International Conference on Embedded Networked Sensor Systems (SenSys), 181-192 (2003).

[37] A. El-Hoiydi: Aloha with Preamble Sampling for Sporadic Traffic in Ad-hoc Wireless Sensor Networksò, ***in Proceedings of IEEE International Conference on Communications***, (2002).

[38] N. Abramson: The ALOHA System ï Another Alternative for Computer Communications, in Proceedings Fall Joint Computer Conference, ***AFIPS Press***, 37: 281-285 (1970).

[39] C.C. Enz, A. El-Hoiydi, J.-D. Decotignie, V. Peiris: ñWiseNET: An Ultralow-Power Wireless Sensor Network Solution, ***IEEE Computer***, 37(8) (2004).

[40] J. Polastre, J. Hill, D. Culler: Versatile low Power Media Access for Wireless Sensor Networks, Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSysô04), Baltimore, MD, (2004).

[41] I. Ramachandran, S. Roy, ñClear channel assessment in energy-constrained wideband wireless networksò, ***IEEE Wãreless Communãcatãons*** 14:70-78, (2007).

[42] M. Buettner, G. Yee, E. Anderson, R. Han, ñX-MAC: A Short Preamble MAC Protocol For Duty-Cycled Wireless Sensor Networksò, (2006).

[43] I. Rhee, A. Warrier, M. Aia, J. Min, ñZ-MAC: a Hybrid MAC for Wireless Sensor Networksò, SenSysô05, San Diego, California, USA, (2005).

[44] B.Tavli, W. Heinzelman, ñMH-TRACE: Multi-hop Time Reservation Using Adaptive Control for Energy Efficiencyò, ***IEEE Journal on Selected Areas in Communicaitons***, 22 :942-953 (2004).

[45] B.Tavli, W. Heinzelman, ñTRACE: Time Reservation Using Adaptive Control for Energy Efficiency***ò, IEEE Journal on Selected Areas in Communicationsò,*** 21:1506-1515 (2003).

[46] B.Tavli, W. Heinzelman, ñQos and Energy Efficiency in Network-Wide Broadcasting: a MAC Layer Perspectiveò, ***Computer Communications,*** 30 :3705-3720 (2007).

[47] T. Numanoĵ lu, B. Tavli, W. Heinzelman, ñEnergy Efficiency and Error Resilience in Coordinated and Non-Coordinated Medium Access Control Protocolsò, ***Computer Communications***, 29 :3493-3506 (2006).