INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET)

ISSN 0976 – 6464(Print)
ISSN 0976 – 6472(Online)
Volume 5, Issue 3, March (2014), pp. 79-93
© IAEME: www.iaeme.com/ijecet.asp
Journal Impact Factor (2014): 7.2836 (Calculated by GISI)
www.jifactor.com

IJECET
©IAEME

# MAC PROTOCOL BASED LOW ENERGY OPERATIONS IN WIRELESS SENSOR NETWORKS

**Rohit D. Gawade**[1], **Dr. S. L. Nalbalwar**[2]

[1,2]Department of Electronics and Telecommunication Engineering,
Dr. Babasaheb Ambedkar Technological University,
Lonere, Raigad, Maharashtra, India

## ABSTRACT

Wireless sensor network is a collection of autonomous, spatially distributed sensor nodes which work together to form a network to monitor environmental conditions such as temperature, pressure, humidity etc. Due to advancement in various technologies like radio, battery and operating systems in sensor nodes, WSN have become an emerging field. For researchers, WSN has become an active area of research due to their wide range of applications in several fields such as agriculture, transportation, military etc. After deployment in remote areas, sensor nodes are generally unattended and have to work with their limited energy resources. Recent advances in WSN have lead to the development of new protocols designed for various applications where energy efficiency is an essential consideration. In WSNs communication among various nodes is achieved by means of unique channel which can be accessed by a single node. To provide shared access of channel among sensor nodes, a medium access control protocol is required to be established. In this paper we provide a comprehensive survey of recent energy efficient medium access control protocols for WSNs. This paper starts with an introduction of wireless sensor networks and discussion of good a WSN-MAC protocol properties. This paper then describes several MAC protocols proposed for sensor networks under two important categories which are schedule based and contention based. The paper concludes with comparison among various MAC protocols regarding various characteristics under each category

**Keywords**: Wireless Sensor Networks, Medium Access Control, Schedule Based MAC Protocol, Contention Based MAC Protocols, Energy Efficient.

## I. INTRODUCTION

A wireless sensor network is used to monitor atmospheric conditions like temperature, pressure, humidity by using various distributed sensors. Data from different sensors are transmitted through multiple hopes to the base station which is located at large distance from nodes. Today wireless sensor networks are having many applications in the military, in agriculture, in transportation, in manufacturing and in smart homes etc. A WSN is made up of nodes which ranges from a few to several hundreds. One or several sensors are attached to each node. Each sensor network node consists of several parts such as internal or external antenna for communication, sensor module for sensor interfacing, digital processor for sensor data processing and a battery to provide energy to node. Each sensor "views" environment. Different physical quantities from environment are mapped into quantitative measurements by using sensors. Sensor nodes send their data to a remotely placed base station. At that base station user can have access to that data [1].

It is very difficult, inefficient and infeasible for humans to monitor physical conditions in harsh environments. Ability of a wireless sensor networks to operate in such atmospheric conditions is the key advantage. In remote and dangerous area sensor nodes can be randomly placed by using various means of transport e.g. sensors can be dropped from helicopters for monitoring physical conditions. Sensor nodes get power from batteries. Battery lifetime is limited. When sensor nodes are placed in remote and dangerous area, they may get damaged. As battery lifetime is limited and nodes may get destroyed while placing, large number of sensors are needed to cover a wide area. Many times hundreds or thousands of sensor nodes are required to monitor a given area. It is necessary to design proper architecture and use better management strategies to operate such huge networks. Nowdays wireless sensor network development process has become an advanced. Due to this earlier wired networks are replaced by wireless sensor networks. WSNs are more beneficial than earlier wired networks as they can be easily placed, their transmission range is more and they can be self organised. These networks are having few drawbacks. Their communication bandwidth is less, storage capacity is small, computational resources, node energy and hence network lifetime is limited. There may be collision among data transmitted by different nodes. To avoid these drawbacks, energy efficient protocols are needed to increase node energy, Media Access Control protocols and routing protocols can be used to avoid collisions among data transmitted by different nodes.

Sensors should be self organized and coordinated to perform the work necessary to support required action. For successful completion of mission for which WSN nodes are placed, communication which is efficient and network layer protocols should be crucially designed. Neighbouring sensor nodes should be connected by communication links for data transfer over multihop wireless sensor network. In wired network sensor nodes are communicated by guided medium whereas in wireless network nodes are communicated by transmitted signal through air in the form of electromagnetic signal. For better sharing of transmission medium by all wireless sensor network nodes a medium access control protocol must be utilized.

This paper is designed to discuss the requirements of medium access control protocol for WSN and to provide survey of the same. In section II background is given. Section III explains basic requirements of media access control protocol. In section IV survey of different media access control protocol used in shared medium is given.

## II. BACKGROUND

A single channel is used for data transmission among different nodes in wireless sensor networks, therefore a single node should transmit a data at a given time to avoid collision. So there is a need of MAC protocols for accessing shared channel without collision. In open system interconnections reference model, datalink layer is subdivided into two sublayers i.e. Logical Link Control (higher) sublayer and Media Access Control (lower) sublayer. MAC protocols are provided by lower sublayer (MAC) of datalink layer and higher sublayer (LLC) supports several MAC options. Physical layer explains how physical devices should process for transmission and reception of bits.

Physical layer handles transreception of bits and encoding and decoding of signals. Above physical layer MAC sublayer is present. MAC sublayer converts data into frames, adds header field and trailer field. At receiver it converts received frame into binary data and provides error detection and correction.

<table>
<tr><td colspan="2">Application</td></tr>
<tr><td colspan="2">Presentation</td></tr>
<tr><td colspan="2">Session</td></tr>
<tr><td colspan="2">Transport</td></tr>
<tr><td colspan="2">Network</td></tr>
<tr><td rowspan="2">Datalink</td><td>LLC Sublayer</td></tr>
<tr><td>MAC Sublayer</td></tr>
<tr><td colspan="2">Physical</td></tr>
</table>

**Fig. 1. OSI reference model**

Communicating nodes are spatially distributed which causes problems in designing effective MAC protocols. It is necessary that each node should know which node can send its data at a given time. For that purpose coordinating must be transmitted to all nodes. Communication channel itself is needed for transmitting that information to all nodes. Such multi-access requirement of communication channel causes access control protocol and overhead required to become more complex. One node cannot get exact information about all other nodes in a network as nodes are spatially separated and any information received by a node is as old as time required for that information to travel through communication channel. Behavioural quality of a multiple access control protocol is mainly dependant on accurate decisions and overhead required by it. Overhead required should not necessarily reduced in order to increase accuracy of decisions made by MAC protocols because decision accuracy may get degrade by reducing overhead. It is very difficult but important to know the information used by MAC protocols. Different MAC protocols use range of information starting from minimum amount to perfect. There are different types of information like predetermined, dynamic global and local. Information common to all communicating nodes is known as predetermined information. While protocol is working, some information is known to few nodes involved in operation, such information is known as dynamic global information. Some information is known to individual nodes which is known as local information. For different nodes to coordinate efficiently and perfectly, predetermined and dynamic global information takes an important part. For communication between different nodes required overhead can be reduced by using local information but may degrade the accuracy of decisions made by protocol[2].

## III. CHARACTERISTICS OF MAC PROTOCOLS

In a MAC layer, a data packet always takes some time before its successful transmission. Such time is known as delay. Traffic in network and designing methods of MAC protocol causes such delay. To meet quality of service requirements of some applications, it is necessary that multiple access control protocols should support delay bound guarantees. A local message within a node and global massage among all nodes in a network must be carefully scheduled to provide delay boundaries which are guaranteed. Delay guarantees are of two types, Probabilistic delay guarantees and deterministic delay guarantees. Probabilistic delay guarantees are given by probabilities and variances. Whenever any massage is arrived, it undergoes different state transitions before it is again transmitted. An ensured predictable number of such state transitions are specified by deterministic delay guarantees. Maximum length of access period is guaranteed by deterministic MAC techniques . Many applications requires their task to be completed within specified time limit. In such environment, deterministic MAC schemes are mainly required.

Communication network transmits massage at a specific rate which is known as throughput which is also an objective of MAC protocol. Unit of throughput is messages per second or bits per second. Fraction of the capacity of the channel used for data transmission is represented by throughput. Whenever communication network has to transmit large amount of data throughput increases initially. When traffic on network reaches certain threshold, the throughput continues to increase or decrease depending on situation. MAC protocols should be designed such that it will minimise massage delay and maximise the channel throughput.

MAC protocol should be reliable and least succeptible to errors which if occurred should detect and mask them. They should have ability to restart and reconfigure network if communicating nodes or links fail.

In WSN size of a network is variable and number of sensor nodes are large exceeding thousands and millions of nodes. Independancy of the communication network on such high number of nodes and variable network size for obtaining desired goals refers to scalability. In order to achieve scalability, use of fixed network architecture should be avoided. Scalability can also be achieved by making structure of communicating network hierarchical like forming clusters from group of nodes and employing strategies which aggregate information from different sensors.

Traffic over a communication network always fluctuates such that it may exceed maximum sustained load with respect to time. A MAC protocol should be able to handle such fluctuations in traffic of the network till network traffic does not become higher than channel capacity. If amount of time taken by packet in MAC layer is within the uppar bound, then protocol is said to be stable by delay. As network traffic increases, if throughput doesnot collapse then MAC protocol is said to be stable by throughput.

If channel capacity demands of all nodes are equivalent, each communication node among all nodes in a network should be allocated an equal channel capacity. In some cases Communication network may contain nodes which demand variable channel capacity. Based on the relative channel capacity demands different weights are assigned to different communicating nodes. Allocating equal channel capacity to all nodes is a difficult task because, to design utilization of a communication channel by all sensor nodes, information known to different nodes during protocol working is required and communication channels of WSNs are time varying.

Sensor nodes get power from low capacity batteries inside it. In WSNs sensor nodes are placed in remote environment. So it is difficult to change node batteries due to which lifetime of a sensor node is reduced. By using low power chips in a sensor nodes, its energy consumption can be reduced. If at a given time two or more sensor nodes transmit its data then collision occurs due to which energy get wasted in resending the data destroyed or corrupted in collision. Whenever a packet is transmitted to any node, there is a possibility that it may get received by some other node. Large energy is used by receiver to receive any packet if transmitter energy is less. To coordinate communication channel access there is need of control packet. If such control packets are transmitted in large amount as compared to the number of data packets, then it causes loss of energy. By reducing rate of change of sensor node i.e. by reducing time interval between active mode and sleep mode of sensor node energy wastage can be avoided [2].

## IV. TRADITIONAL MAC PROTOCOLS

The capability of a wireless sensor network depends on type of media access control protocol used for it. Various nodes in WSN can access communication channel by different ways. Most common strategies includes fixed access strategies and random access strategies.

**Fixed assignment strategies:** In fixed assignment protocols, irrespective of the need, channel assignment is fixed. In this strategy, each node can use its resources exclusively such that collisions will not occur. There are two types of fixed assignment strategies which include long term fixed assignment protocols and short term fixed assignment protocols. For long term fixed assignment strategies duration of channel assignment is for minutes, hours etc whereas for short term fixed assignment strategies, wireless channel is assigned to communicating nodes for very short duration of time like milliseconds or tens of milliseconds. Due to such channel assignment for very short duration data bursting may occur. Due to fixed channel assignment, it becomes very easy to implement such protocols. In WSNs many devices need variations in channel assignment. Such communication variations needs are neglected by fixed fixed assignment protocols. If network condition is varying oftenly because of changes occurred in topology, dying and newly forned nodes, changing data transmission patterns, it becomes inflexible to implement fixed assignment protocols. Because of such temporary and self creating nature of WSNs, fixed assignment channel access protocols are used for them in rare cases. To reform channel assignment to nodes used in varying network configurations, signalling techniques are required in fixed assignment protocols.

Typical protocols that include this strategy are Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), Space Division Multiple Access (SDMA).

**TDMA:** In TDMA, entire radiofrequency spectrum is divided into different time slots and each node is allowed to transmit and receive its data during that time slot. All time slots forms one frame and channel is considered as a time slot that repeats in each frame. Each TDMA frame contains preamble, an information message and trail bits.

| Preamble | Information Message | | | Trail Bits |
|---|---|---|---|---|
| | Slot 1 | Slot 2 | Slot N | |

**Fig. 2a. TDMA Frame Structure**

| | | | |
|---|---|---|---|
| Trail Bits | Sync. Bits | Information Data | Guard Bits |

**Fig. 2b. Time Slot**

Addresses required by transmitter and receiver to identify each other is specified in preamble. Synchronisation of receiver between different time slots is provided using guard bits. Half of time slots in information message is used for transmission and remaining are used for reception so duplexers are not required. Any node transmits its data in buffer and burst method i.e transmission is discontinues due to this high synchronisation bits are required in TDMA systems[3].

**FDMA:** In FDMA system, a unique frequency band is allocated to each node as a communication channel. Individual nodes who request for resources get individual channel on demand. No other node can use that channel during data transmission. Two frequencies are assigned as a communication channel to individual node. One is for forward path and another is for reverse path. Once channel is established, transmitter and receiver can operate simultaneously. In FDMA, data transmission is continuous hence less synchronisation bits are required as compared to TDMA system. Due to simultaneous working of transmitter and receiver, duplexers are required which increases cost [3].

**CDMA:** Various sensor nodes can transmit their data simultaneously by using code division multiple access technique which is a spread spectrum based scheme. In spread spectrum technique, binary data to be transmitted is given to the channel encoder. At the output of channel encoder, an analog signal is produced with one centre frequency and its bandwidth is limited around that frequency. This modulated signal is transmitted over communication channel alongwith spreading code which is digit sequence generated by pseudorandom generator. Because of this spreading code, the bandwidth of the transmitted signal becomes very high as compared to original signal. The received signal is demodulated using same spreading code.

Mainly there are two types of spread spectrum techniques: Frequency Hopping Spread Spectrum and Direct Sequence Spread Spectrum. In frequency hopping spread spectrum multiple channels which are formed by different carrier frequencies are assigned to input signal. $2^k$ channels are formed by $2^k$ carrier frequencies. Spreading code decides sequence of channels used because each k bit of the spreading code decides one of the $2^k$ carrier frequency. Transmitter uses one channel at a time for fixed time interval. During that time interval binary bits which are encoded by using digital to analogue encoding scheme are transmitted. The received signal is again demodulated by frequencies decided by spreading code to produce output data[4].

In direct sequence spread spectrum each input bit which is to be transmitted is represented by multiple bits using spreading code e.g. input bit 1 can be represented by spreading code <1 0 0 1>, and 0 can be represented by using spreading code <0 1 1 0>. Depending upon number of bits used in spreading code, input signal is spread over wide range of frequency. Four bit spreading code will spread input signal over frequency band which is four times higher than one bit spreading code. Input bit stream is combined with spreading code using exclusive –OR e.g. in above example input bit 1 is Ex-ORed with each bit in its spreading code to form a bit sequence < 1 0 0 1> which is transmitted over communication channel. In similar way, input bit 0 is transmitted as <0 1 1 0>. At receiver received bits are again XORed with spreading code identical to that used at transmitter to receive original input information [4].

**SDMA:** In Space Division Multiple Access technique, Central base station contains spot beam antennas which control radiated energy for all nodes in networks. Spot beam antennas may use same frequency or different frequencies for various nodes covered in their area. When same frequency is to be used for different nodes present in the network, then TDMA or CDMA has to be employed. If frequencies need to be use are different, then FDMA technique should be employed. Nodes should be physically separated by sufficient distance to avoid cochannel interference which limits number of nodes in the network[3].

**Demand Assignment Strategies:** In fixed assignment channel access protocols, capacity of a channel is assigned to all nodes in the network irrespective of their needs. In demand assignment strategies, channel capacity is allocated to communicating nodes in optimum fashion. All nodes which are in idle state are neglected by demand assignment protocols and nodes which are ready to transmit are only taken into consideration while channel capacity assignment. Time for which channel is allocated to communicating nodes depends on time that nodes require to transmit a packet.

Network control mechanism is required to provide arbitrary access of the communication channel to communicating nodes. When any nodes need to have access to the communication channel, it should send request by using logical control channel other than data channel. There may be delay in data transmission because of request for channel access. Demand assignment channel access methods are again classified into two types, centralised control and distributed control [2] .

**Centralised Control**: In a centralized control, Central controller sends query massage in some specific order, whether any communicating node has a data to transfer. If node is intended to transmit its data, it accepts query message sent by central controller. Once query request is accepted, central controller, channel is allocated to ready mode by controller to transmit nodes data at full data rate.

Node rejects controller request if it does not have data to transmit. After rejection, controller transmits its query message to another node in the network. Few nodes which have large amount of data to transfer are often polled by central controller however all nodes get equal access to communication channel. Controller generates many messages to query all nodes in the network, due to which large overhead is required which is limitation of centralised control strategy of demand assignment channel access protocols.

**Distributed Control:** Some time slots are used for carrying reservation messages in distributed control scheme. Reservation messages are called minislots as they are smaller than data packets. When any nodes wants to transmit its data, it sends reservation message to the central controller using reservation minislot. Usually unique minislot is assigned for each user whereas in some cases nodes sends request to have access to minislot. Controller declares a transmission schedule for requesting user after reception of its request. Collision can be avoided by providing unique reservation minislot to each user or by scheduling urgent data before delay insensitive data by controller [2].

### Random Assignment Protocols

In FDMA scheme, a frequency band, and in TDMA scheme, a time slot is allocated to each communicating node. Even though node doesn't have a data to transmit, channel sources are assigned to communicating nodes. Bandwidth allocated is wasted if node doesn't have any data to transmit. Bandwidth is not preallocated to communicating nodes, in random assignment strategies.

Communication channel should be accessed by which communicating node is not decided by random access protocols also time required for any node to transmit is not assigned by random assignment strategies. If two or more nodes transmits data at a same time, collision can occure. Random assignment protocols must include collision detection mechanism and retransmission scheme for collided packets. Some random assignment protocols includes, ALOHA, Slotted ALOHA, CSMA/CD (carrier sense multiple access with collision detection), CSMA/CA (carrier sense multiple access with collision avoidance).

**ALOHA:** ALOHA is used to provide shared communication channel access to users which are not coordinated. In ALOHA, whenever a node is ready to transmit a data, it is simply allowed to transmit. Transmitting communication node listens for some period once it completes data transmission. Time for which transmitting communication node listens is equal to the time required for data to travel between two nodes which are farthest apart from each other in the network.. Once data is received by receiver node, it examines the error checksum to verify whether data is correct. After verifying the correctness of data, receiving node sends an acknowledgement. Successful transmission occurs if, before the completion of time for which transmitting node listens, it receives acknowledgment. If noise is present in the communication channel, or if collision occurs, then data is lost and acknowledgement is not generated. Nodes can be added or removed easily in the network as no central control is present in ALOHA. When traffic is less nodes can get access to communication channel in short period of time. Drawback of ALOHA is that, when traffic is high, collisions are rapidly increases due to which degradation of network performance takes place [7][8].

**Slotted ALOHA:** Channel is divide into equal length time slots which are having higher length than duration of packet. In Slotted ALOHA, packets are distributed in discrete manner i.e. only at the beginning of a new time slot, each node transmits a massage. Collision of one packet with portion of another is avoided in this strategy. If complete collisions occur, packets get destroyed which are need to transmit again if number of users increases. Traffic delay characteristics are determined by the number of time slots for which any node waits before retransmitting packets lost in collision [3].

**CSMA:** ALOHA protocol cannot get information about other nodes in the network because sender doesn't listen for channel before transmission. Greater output can be obtained if, before transmission, channel is listened by transmitter. In CSMA protocols, before transmitting information, each node in the network is able to listen channel condition. Based on specific algorithm, sender is made to send data, if channel is idle. Time required by a node to sense whether the channel is idle or not is known as detection delay [3]. CSMA protocols are divided into two categories non persistent CSMA and persistent CSMA. In non persistent CSMA protocol, before transmission, sender senses channel to determine if another node is transmitting data. Sender waits for an acknowledgement after transmitting data if channel is idle. If noise is present on channel or if collisions occurred then data gets lost and sender cannot receive acknowledgement. Packet retransmission is scheduled by sender in such cases. Sender nods goes into back off mode if channel is found busy for random amount of time. This process is repeated till successful data transmission is occurred. The major limitation of non persistent CSMA is that, when sender node is back off, channel may remain idle which causes overall throughput reduction due to channel capacity wastage. To eliminate the limitation of nonpersistent CSMA, P-persistent CSMA protocols are developed. In 1-persistent CSMA scheme a node first sense a channel if is ready to send packet, Node transmits its packet if channel is free. If busy channel is sensed, till channel becomes idle, node persistently continues to listen. When channel is sensed as idle, sender node transmits its data.

In p persistent CSMA, Probability that sender node sends data after sensing idle channel is p and probability that sender waits for specific time period before trying to transmit packet again is 1-p. Time for which sender waits before transmitting packet is equal to the time required for packet to travel between two nodes which are farthest apart from each other in case of unslotted ALOHA or time slot in case of slotted ALOHA. Node again sense channel after completion of waiting period. Node continues to listen again if channel is sensed as busy. If channel is sensed as idle, node transmits its packet with probably of p.

There are few drawbacks of CSMA based scheme. Even after collision occurs, sender node continues to transmit data packet. Each node has to wait till previous packet is transmitted successfully before sending new packet. These drawbacks of CSMA based schemes are avoided if communicating node, while transmitting data, is able to listen channel which is provided by CSMA/CD protocol [2].

**CSMA/CD:** In CSMA/CD based scheme, when collision occurs, node is able to detect it by monitoring signal on the channel. Sender node first determines if any other node is transmitting its packet over the communication channel by listening the channel. If no other node is transmitting a packet over communication channel, then sender starts transmitting its data and while transmitting, it continuously listens a channel. Sender node stops its transmission immediately if other interfering signal is detected over communication channel. This saves the amount of bandwidth required for transmitting signal after detection of collision. Sender node waits for a random amount of time before transmitting packet again after detection of collision. As distance increases, signal power is reduced also wireless channels are time varying due to which it becomes difficult for sender node to determine whether collision is present or not at the receiver node which limits the use of CSMA/CD strategy [2].

**CSMA/CA:** Carrier sense multiple access collision avoidance makes use of RTS (Request to send), CTS (Clear to send) handshake to avoid collision. Suppose that node A wants to transmit a data packet to node B. Sender node A first monitors a channel to determine if any other node is transmitting data over that channel. If channel is found as idle, sender node A transmits a RTS packet to all other nodes in the communication range of node A. The RTS packet contains destination address and time required for data packet transmission completion and acknowledgement reception.

All nodes in the communication range of node A except node B avoids transmitting their data after receiving RTS packet by node A till data transmission is completed successfully between node A and B. After receiving RTS packet by sent by node A, node B transmits a CTS packet to all nodes in the communication range of node B. CTS packet contains time remained for data transmission completion between node A and node B. After receiving CTS packet sent by node B, all nodes in the communication range of node B except node A avoids data transmission till successful transmission occurs between node A and B. After receiving CTS packet sent by node B, node A starts transmitting its data to node B. When node A completes transmitting data to node B, node B sends acknowledgement which indicates data is transmitted successfully form node A to node B [2].

## V. MAC PROTOCOLS FOR WSNs

When a node receives a packet intended for other sensor nodes, energy consumption is increased in receiving and decoding those packets. After realising that these packets are not destined to that particular node which receives them, those packets are dropped. When any node listens to a channel for large amount of time, again energy consumption is increased. When two or more sensor nodes attempt to transmit simultaneously, collision may occur Retransmission of such colliding packets is yet another source of significant energy wastage. Such excessive power consumption leads to degradation of MAC layer protocol performance. Reduction of the wastage of energy caused by such reasons is the main aim of MAC protocols. There are two types of MAC protocols, schedule based and contention based MAC protocol. In schedule based MAC protocols, schedule decides access of channel to all nodes. Channel is preallocated to individual sensor nodes and at a one time channel is accessed by one sensor node. Preallocation of resources to individual sensor node is avoided in contention based MAC protocols. All nodes can access single communication channel on demand. If multiple nodes tries to access channel at a same time, collisions may occur which should be minimized or completely avoided in contention based MAC layer protocols. Communicating nodes should access to channel based on distributed and randomized algorithms which can be rescheduled to eliminate collision. To avoid energy wastage caused by listening packets destined to other sensor nodes, node goes into sleep rate when they become inactive.

### Schedule Based MAC Protocols

Schedule based MAC protocols uses time slots, frequency bands or spreading code as used in CDMA as communication channel. Variant of TDMA scheme, where channel is divided into different time slots are used by many schedule based protocols. One frame is repeated cyclically over time which is logically formed by a set of N time slots. For working of sensor node in each logical frame, a schedule is formed by assigning a set of specific time slots to each sensor node. Based on that schedule, a sensor node alternates between two modes of operation i.e. active mode and sleep mode. In particular time slot which is assigned to a sensor node, it goes into active mode where sensor transmits and receives data frames. Outside of the time slot which is assigned to that sensor node, it goes into sleep mode in which radio trans receivers are off to conserve the energy.

### Self Organising Medium Access Control Protocol for Sensor Networks (SMAC)

In SMAC for communication with known neighbours, a superframe, which is a TDMA like frame having fixed length is maintained by each node in a network. Super frame consists of smaller frames having size variable in time for a single node. In self organizing media access control protocols, Neighbouring nodes are detected by executing a neighbourhood discovery procedure. Each node assigns a unique time slot to link connecting that node to each neighbour node. Time slots should be selected such that in each time slot node can talk only to its neighbours. Since node and its neighbours can transmit a data in a same time slot, interference between neighbour links is avoided by proper link establishment procedure. To achieve this, FDMA technique or spreading code as used in CDMA technique is assigned to each link. Each node has its own schedule of time slots with all its neighbours by using super frame structure. Radios of nodes should be tuned to proper frequency channel if FDMA technique is used or spreading code if CDMA technique is assigned to channel.

**Bluetooth**

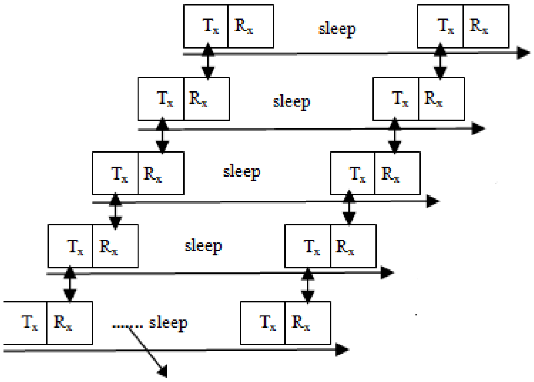
Piconet is known as a group of devices sharing a common channel. For controlling channel access of at most seven group participant slave devices, master unit is present in each piconet. 625-ms slots forms one channel. 48 bit Bluetooth device address of master and clock determines a unique frequency hopping pattern assigned to each piconet. Frequency hopping sequence assigned to each piconet is followed by all slave devices in that piconet. Bridge nodes can be used to connect piconets to each other to form scatternets which are larger adhoc networks. A unique 3 bit internal address is assigned to each slave device by master within piconet. A slotted time division duplex protocol, in which time slots are allocated to slave nodes by master with the help of polling protocol is used to regulate access to the channel. Piconet master and slave can exchange packet in two time slots which forms a Bluetooth frame. Slave devices are polled by master continuously for communication. If master addresses a slave in one time slot, then slave can communicate in next time slot [2].

**TRAMA (Traffic Adaptive Medium Access)**

For achieving collision free channel and energy efficiency, a TDMA based protocol, known as Traffic Adaptive Medium Access( TRAMA) has been designed. In this protocol, collision free transmission is ensured and when nodes are not transmitting or receiving, they are switched to low power idle state to reduce wastage of power. It assumes time synchronization of nodes and time is divided into cycles and each cycle consists of random access and schedule access periods. When channel access is contention based, In order to establish two hope topology information random access period is used. TRAMA consists of three main parts, neighbour protocol, schedule exchange protocol and adaptive election algorithm. For information collection of neighbouring nodes, the neighbour protocol is used. To exchange two hope neighbour information, by using small timeslots which are randomly selected, the schedule exchange protocol is used. Using neighbourhood and schedule information, in order to decide the transmitting and receiving nodes, an adaptive election algorithm is used. A current schedule is transmitted to neighbour by schedule exchange protocol. By using random access phase, neighbours schedule can be received by node. Node decides which slot from schedule access phase can be used by using neighbour schedule information. For this time slot selection, each node, by using global hash function h calculates priority P for its node identifier X for each time slot. Priority P is given by P(x,t) = h(x©t) where x©t is the concatenation of x with current time t. Each node calculates its priority. X transmits its packets in the time slot for which X has highest priority value among all its two hop neighbours [5] [6].

**Data Gathering MAC (D-MAC)**

For tree based data gathering, a schedule based MAC protocol, known as data gathering medium access control protocol is designed in wireless sensor networks. This protocol is mainly designed to maintain energy efficiency while achieving low latency. This protocol uses small time slots and within each slot, uses carrier sense multiple access with acknowledgement for transmission and reception of one packet. Communicating node uses one slot for transmission, one slot for reception and n slots for sleep mode. If at a depth of n in the tree, source node is present, it transmits single packet to the sink node with n time slots delay which is of the order of tens of milliseconds [5]. In order to solve the interface problem between nodes on different branches of tree, D-MAC uses an MTS (More to Send) control packet. If channel is busy, node cannot send its packet. In such case, node sends request MTS packet to its parent node in data gathering tree for waking up one receiving slot time earlier [6].



More active slots if necessary

**Fig. 3. DMAC in data gathering tree**

### Contention based Protocols

Protocols for which channel access among all nodes does not require any coordination among them is known as contention based protocol or random access based protocols. Before attempt to access channel, for a random duration of time colliding nodes goes into back off state. To make these protocols robust and to improve their performance, RTS (request to send) and CTS (clear to send) mechanisms and collision avoidance techniques are used along with these protocols. Due to large overhead requirement, idle listening, collision and overhearing, there are limitations on energy efficiency of contention based MAC layer protocols. Random access MAC layer protocols should be designed in order to reduce the energy waste for extending the network lifetime.

### PAMAS (Power Aware Multi-access Signalling)

In order to achieve energy efficiency, one of the earliest contention based MAC protocol designed is Power Aware Multi-access Signalling protocol. Two separate signalling channels for the data and control packets are used by this protocol due to which overhearing is avoided among neighbouring nodes. In PAMAS, nodes which are not transmitting or receiving are turned “OFF” by combining the use of a busy tone with RTS and CTS packets. At each sensor nodes, two radios in different frequency bands are required due to which design complexity, size and cost of sensors is increased. Node switches between sleep and wake up state rapidly due to which significant power consumption occurs. Idle listening causes energy wastage which cannot be reduced by PAMAS protocol [9][10].

### STEM (Sparse Topology and Energy Management)

Sparse topology and energy management protocol uses two radio channels, a wake up radio channel and a data radio channel. For wake up signal, instead of encoded data, busy tone is used by a variant of STEM. In STEM protocol, till communication with any node is desired, one node turns off its data radio channel. Node transmits data on a wake up radio channel, when it has a data to transmit. Wake up signal channel acts like a paging signal. Till all neighbouring nodes are paged, transmission of this signal lasts. Nodes may remain awake for long period after it awakes from its sleeping mode, to receive “session” of packets. Before going into sleep mode, node can also awaked to receive all its pending packets. Wastage of energy occurs in continues transmission of wake up signals if frequent events are occurred [11].

### Timeout-MAC

To communicate with each other, in timeout-MAC, node use RTS and CTS acknowledgement packet to ensure reliable transmission and avoid collision. To adapt traffic load variations and to reduce energy consumption, an adaptive duty cycle is used by this protocol. All messages are transmitted in variable length burst to avoid idle listening. Between burst, nodes are allowed to sleep. During the active period, node keeps listening and frame which contains messages stored in buffer are transmitted. For a predetermined time interval (Ta), when no active event occurs, an active period ends. Time interval after which active period ends is equal to sum of contention interval length, RTS packet length, time interval between the end of the RTS packet and the beginning of the CTS packet, CTS packet length.

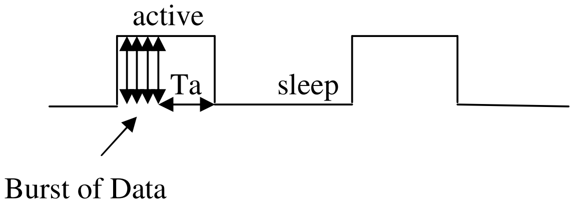


**Fig. 4. T-MAC Scheme**

Active event includes reception of data over the radio, hearing of a periodic frame timer, collision sensing on the channel. The node goes into sleep mode at the end of the active period [12].

### B-MAC ( Berkeley- Media Access Control)

B-MAC is designed for N sender to 1 receiver transmission in an adhoc networks of nodes. Periodically sleep/wake up cycles are used by B-MAC protocol. This protocol uses LPL (Low Power Listening) mechanism. In this mechanism, node listens for incoming data transmission in the wake up time. If “false positive” occurs i.e. no data is received, listen state is interrupted by timeout otherwise node waits for a complete packet transmission. After wake up, to verify the completion of packet reception from the beginning, a 100 ms preamble time is added. LPL doesn’t guarantee fairness. For different nodes, sleep period can be different. Node starts to send an announcement by switching radio mode when node has a data to send. Even if receiver starts sleeping at the beginning, this announcement should be long enough so that receiver can notice. After that sender sends target address and data transmission starts. B-MAC uses clear channel assessment (CCA) to reduce amount of needed energy and clear channel detection [13].

### S-MAC (Sensor MAC)

For wireless sensor networks, S-MAC which is a contension based protocol inherited from CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is designed. To avoid energy wastage and idle listening, S-MAC uses periodic “Listen and Sleep” method in which a periodic listen and sleep schedule is followed by each node. In listen period, the network is sensed by the node. If network is found idle, node listens and communicates with other nodes. In sleep period, nodes turn off their radios and try to sleep which reduces wastage of time during idle listening also avoids large amount of energy consumption caused by unnecessary idle listening. In S-MAC node uses RTS (Request to Send), CTS (Clear to Send) and Data Acknowledgement (ACK) for communication. Node goes into sleep mode after finding a RTS or CTS packet destined for some other node. Once sleep mode is completed node enters into wake up mode and search for an event. Node again goes into sleep mode if an event is not found. Synchronisation schedule for sleep and listen period is shared by broadcasting SYNC packet to neighbouring nodes which forms a virtual cluster. Due to this, a network may contain multiple clusters. If two neighbouring nodes are present in two different virtual clusters, they may follow two different schedules of those respective virtual clusters i.e. during listen periods of both clusters, they may wake up which causes energy wastage by idle listening and overhearing.  Basic S-MAC scheme is shown in figure below in which. In figure below, node 1 transmits data to node 2 [14].

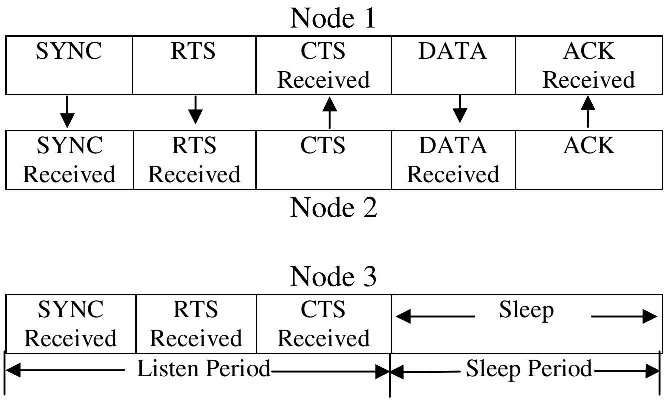


**Fig. 5. S-MAC Scheme**

**WiseMAC**

WiseMAC is a nonpersistent CSMA and preamble sampling technique based medium access control protocol developed for wireless sensor networks to reduce consumption of power. WiseMAC protocol represents an extension of Aloha with preamble sampling. In Aloha with preamble sampling, for listening the channel, node wakes up from sleep mode. A node listens to the channel for a constant duration of time known as sampling period independently. If channel is listened as free, till next time slot appears, node goes back to sleep mode. A sender node sends a long dummy packet, called preamble having size equal to sampling period in front of every data frame to avoid missing the neighbours wake up schedule. After wake up, when node detects preamble, it continues to listen channel till valid data is received. By using an acknowledgement frame (ACK), the reception of valid message is confirmed. A biggest disadvantage of preamble sampling is that all receivers have to receive the long preamble even if they are not addressed. WiseMAC tries to use minimum sized wake up preamble. In WiseMAC sender transmits packet shortly before the receiver is expected to wake up. To preserve the energy, sender can go in sleep mode during this time. When receiver wakes up, it can detect the preamble and it remains in wake up mode till data is received. Once data is received successfully, an ACK frame is transmitted by the receiver.The WiseMAC ACK packet carries acknowledgement information as well as information for other nodes including sender about the remaining time of next sampling. This time is stored by other nodes in their table. By using this information, a node can determine the wake up intervals of all its neighbours and transmit a packet with minimized size of preamble [15] [16].

## VI. CONCLUSION

In recent years, MAC protocols in WSNs have attracted large attention and introduced unique challenges as compared to traditional MAC protocols in other wireless networks. Several MAC protocols for WSNs have been proposed by researchers. In this paper survey of schedule based and contention based MAC protocols for WSNs has been presented.

Collision can be avoided by using TDMA technique. TDMA technique uses idle slots due to which when less data is to be transmitted, throughput is reduced and clock drift problem arises.

Synchronisation of nodes and ability to handle topology changes are critical issues in TDMA because of insertion and deletion of new nodes. In FDMA technique cost of sensor nodes increases due to requirement of an additional circuitry for communication with different radio channels which is a major drawback even though it allows collision free access to medium. CDMA technique also avoids collision while giving access to channel but requirement of computational complexity increases energy consumption and cost of sensor network. In order to reduce the computational complexity, several techniques like use of simple modulation schemes and design of simple receiver models are adopted. In CSMA/CA channel is listened by nodes all the time due to absence of sleep periods due to which power is highly consumed.

In Schedule based protocols, TRAMA and DMAC can automatically adapt scheduling to varying traffic load whereas SMAC provides less traffic adaptively. Ability to handle changes in network topology is moderate to high in SMAC and TRAMA whereas DMAC provides less adaptivity to changes in topology. SMAC and TRAMA provides high latency in time as compared to DMAC.

Simulation results show that in SMAC,when any node detects RTS, CTS packet destined to other node, it goes into sleep mode due to which under high traffic conditions power consumption decreases. SMAC provides fixed duty cycle to all nodes. When traffic load is high to avoid dropping of messages a large value duty cycle must be selected which reduces idle listening and power consumption. SMAC achieves acceptable results when low power listening is used. When T-MAC is used with LPL it produces better results regarding power consumption and network lifetime as compared with SMAC. In terms of power consumption simulations show that WiseMAC provides best results as compared to other MAC protocols.

The paper begins by introducing wireless sensor networks and characteristics of MAC protocols used in general wireless networks. We have briefly described four schedule based and six contention based MAC protocols for WSNs. Finally we have compared performance of various schedule based and contention based MAC protocols for achieving certain requirements. Though many MAC schemes have been proposed for WSNs, there is no standard MAC protocol because MAC protocol depends on certain application. We expect that this survey will help researchers in selecting MAC protocols for WSNs in order to achieve satisfactory results in certain application.

## REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_sensor_network.

[2] Kazem Sohraby, Daniel Minoli, Taieb Znati, “Wireless Sensor Networks Technology, Protocols, and Applications” A John Wiley & Sons, INC., Publication.

[3] Theodore S. Rappaport, “Wireless Communications Principles and Practice” Second Edition Prentice Hall India.

[4] William Stallings, “Wireless Communications and Networks,” Upper Saddle River, NJ 07458.

[5] Rajesh Yadav, Shirshu Varma, N. Malaviya, “A Survey of Mac Protocols for Wireless Sensor Networks”, UbiCC Journal, Volume 4, Number 3, August 2009.

[6] Abul Kalam Azad, M. Humayun Kabir, Md. Bellal Hossain, “A Survey on Schedule-Based MAC Protocols for Wireless Sensor Networks”, International Journal of Computer Science and Network, Volume 2, Issue 6, November 2013.

[7] F. A. Tobagi, L. Kleinrock, ‘‘Packet Switching in Radio Channels: Part II: The Hidden Terminal Problem in Carrier Sense Multiple Access and the Busy Tone Solution,’’ IEEE Transactions on Communications, Vol. 23, Dec. 1975, pp. 1417–1433.

[8] L. Kleinrock, Fouad Tobagi, ‘‘Packet Switching in Radio Channels, Part I: Carrier Sense Multiple Access Modes and Their Throughput Delay Characteristics,’’ IEEE Transactions on Communications, Vol. 23, No. 12, Dec. 1975, pp. 1400–1416.

[9] S. Singh, C. S. Raghavendra, ‘‘PAMAS: Power Aware Multi-access Protocol with Signalling for Ad Hoc Networks,’’ ACM Computers in Communications Review, Vol. 28, No. 3, July 1998, pp. 5–26.

[10] 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).

[11] C. Schurgers, V. Tsiatsis, S. Ganeriwal, M. Srivastaval., ‘‘Optimizing Sensor Networks in the Energy-Latency-Density Design Space,’’ IEEE Transactions on Mobile Computing, Vol. 1, No. 1, Jan.–Mar. 2002.

[12] T. V. Dam, K. Langendoen, ‘‘An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks,’’ Proceedings fo the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys’03), Los Angeles, Nov. 2003.

[13] J. Polastre, J. Hill, D. Culler, ‘‘Versatile Low Power Media Access for Wireless Se nsor Networks,’’ Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys’04), Baltimore, MD, Nov. 2004.

[14] Smriti joshi, Anant Kr. Jaiswal, Pushpendra Kr. Tyagi, “A Novel Analysis of T Mac and S Mac Protocol for Wireless Sensor Networks Using Castalia”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[15] Philipp Hurni · Torsten Braun · Markus Anwander, “Evaluation of WiseMAC and extensions on wireless sensor nodes,” ©Springer Science+Business Media, LLC 2009.

[16] C. C. Enz, A. El-Hoiydi, J-D. Decotignie, V. Peiris, “WiseNET: An Ultralow-Power Wireless Sensor Network Solution”, IEEE Computer, Volume: 37, Issue: 8, August 2004.

[17] Mohamed Elhawary and Zygmunt J. Haas, Fellow, IEEE, “Energy-Efficient Protocol for Cooperative Networks”, IEEE/ACM Transactions on Networking, Vol. 19, No. 2, April 2011.

[18] Neeraj Tiwari, Rahul Anshumali and Prabal Pratap Singh, “Wireless Sensor Networks: Limitation, Layerwise Security Threats, Intruder Detection”, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 2, 2012, pp. 22 - 31, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.

[19] Mr.Yogesh V Patil, Mr. Pratik Gite and Mr.Sanjay Thakur, “Automatic Cluster Formation and Assigning Address For Wireless Sensor Network”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 4, 2013, pp. 116 - 121, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[20] Preetee K. Karmore, Supriya S. Thombre and Gaurishankar L. Girhe, “Review on Operating Systems and Routing Protocols for Wireless Sensor Networks”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 331 - 339, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[21] Yogesh V Patil, Pratik Gite and Sanjay Thakur, “Automatic Cluster Formation and Assigning Address for Wireless Sensor Network”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 4, 2013, pp. 116 - 121, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[22] Basavaraj S. Mathapati, Siddarama. R. Patil and V. D. Mytri, “Power Control with Energy Efficient and Reliable Routing MAC Protocol for Wireless Sensor Networks”, International journal of Computer Engineering & Technology (IJCET), Volume 3, Issue 1, 2012, pp. 223 - 231, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.