Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.11, 2015
www.iiste.org

Working Principles and Performances Analysis of IEEE 802.11 and Sensor s-MAC

Bushra Rahman Md Rafiqul Islam
Lecturer, Department of Computer Science & Engineering, City University, Bangladesh

Abstract
Wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices which use large amount of energy consuming battery-powered sensors to monitor physical or environmental conditions. Medium Access Control (MAC) protocols play a big role to reduce energy consumption in WSN. Designing power efficient MAC protocol prolongs the life time of the network, can consume little power, and avoid collisions from interfering nodes. MAC protocol use scheduler to check if the MAC layer needs to perform any tasks. Contention based MAC protocols relax time synchronization requirements and can easily adjust to the topology changes. IEEE 802.11 and S-MAC are two contention based MAC protocols. In this paper, after describing working principles and limitations of IEEE 802.11 and S-MAC we discuss their energy efficiency and then run a simulation by NS-2 simulator with different number of nodes to compare the throughputs given by IEEE802.11 and S-MAC.
Keywords: WSN, IEEE 802.11, S-MAC, Schedule

1. Introduction
Medium Access control (MAC) protocols are designed in such a way that can consume little power, avoid collisions from interfering nodes, can be implemented with a small code size and memory requirements, changing frequency. This technique ensures how nodes share the channel and do the successful network operation. The MAC protocols for the wireless sensor networks can be classified into two categories: Schedule based which maintains strict time synchronization by scheduling transmit & listen periods and Contention based which relaxes time synchronization requirements and can easily adjust to the topology changes. SMAC is one of the contention based protocols which is the modification of another MAC protocol IEEE 802.11. In this paper we work with IEEE 802.11 and SMAC. The paper is organized as follows: Section II explains designing a well-defined MAC protocol. In section III, working principles of IEEE802.11 & in section IV working principles of SMAC are described with their limitations. Section V and VI describe the performances and simulation result. Finally, the conclusion is outlined in section VII.

2. Designing a well-defined MAC protocol
For designing a well-defined MAC protocol first we have to know about the communication pattern to transmit data in WSN. Different kinds of traffic like: broadcast communication, local gossip, converge cast etc. are used to transmit data. Then we have to avoid the sources of energy wastages in MAC protocol which are happened for sharing a common channel. Reasons for energy wastage in WSN are: Collision of packets, Overhearing, Control packet overhead, Idle listening, Over-emitting etc. Then we have to ensure the attributes of a well-defined MAC protocol. They are: efficiency of energy savings, throughput of the network, scalability and adaptability, self-stabilization, avoiding collision, hidden and exposed terminal problems etc.

2.1. IEEE 802.11
The IEEE 802.11 is a contention based medium access control protocol which uses carrier sensing and randomized back-offs to avoid collisions of the data packets during transmission.
Working principle of IEEE 802.11:

- Acknowledgement (ACK) frame: After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- Request to Send (RTS) frame: The RTS and CTS frames provide an optional collision reduction scheme for access points with hidden stations. A station sends a RTS frame to as the first step in a two-way handshake required before sending data frames.
- Clear to Send (CTS) frame: A station responds to an RTS frame with a CTS frame. It provides clearance for the requesting station to send a data frame. The CTS provides collision control management by including a time value for which all other stations are to hold off transmission while the requesting stations transmits. The IEEE802.11 MAC protocol has two modes: DCF & PCF.
- The DCF defines two access mechanisms for packet transmissions: basic access mechanism and RTS/CTS access mechanism.

- Basic access mechanism follows carrier sensing & virtual carrier sensing mechanisms.
  In carrier sensing, if medium is idle, the node transmits the data frame. If the medium is busy, the node waits until it becomes idle again. The receiver node answers with an ACK (acknowledgment) control frame, upon frame reception. If a collision occurs, transmitting nodes wait a random time and try again and again.

In virtual carrier sensing, any station, before transmitting a DATA frame, senses the channel for duration of time equal to the Distributed Inter-frame Space (DIFS) to check if it is idle. If the channel is determined to be idle, the station starts the transmission of a DATA frame. All stations which hear the transmission of the DATA frame set their Network Allocation Vector (NAV)(An indicator, maintained by each station, of time periods when transmission onto the wireless medium (WM) will not be initiated by the station.) to the expected length of the transmission, as indicated in the Duration/ID field of the DATA frame. Upon successful reception of the DATA frame, the destination station waits for a SIFS interval following the DATA frame, and then sends an ACK frame back to the source station indicating successful reception of the DATA frame. The channel is considered to be busy if either the virtual carrier sensing indicates. In that case, the station enters into a wait period.

- The RTS/CTS access mechanism uses a four-way hand shake in order to reduce bandwidth loss due to the hidden terminal problem. The four way handshake prevents any DATA-DATA collisions that might occur due to the hidden terminal problem.
- PCF is a special node called the access point (AP), polls every node to control the communication process. Periodically, an AP broadcasts a beacon control frame with parameters and invitations to join the network.

Some Limitations of IEEE802.11:

- IEEE802.11includes the large overhead in control and data packets. 802.11 requires 34 bytes for the header and the checksum, TCP and IP require a minimum of 20 bytes for each header, so there is at least 74 bytes of overhead to send application information, which in WSNs may be only two bytes.
- The most important problem for using 802.11 in WSNs is energy consumption since it does not address the issue of avoiding overhearing and idle listening. Although this standard has power saving mechanisms, according to Ferrari et al. “power consumption is rather high, and the short autonomy of a battery supply still remains the main disadvantage of the proposed IEEE802.11 sensor system” [6].
- In transmitting a long message using a single data packet through a lossy channel is hazardous and risky. Even when a few bits in the packet are corrupted during the transmission, the whole packet must be re-transmitted. One of the most common problems of IEEE 802.11 is hidden terminal problem. There two nodes that are outside each-other’s range perform simultaneous transmission to a node that is within the range of each of them, hence, there is a packet collision. The reason for this problem is the broadcast nature of the radio channel, namely, all the nodes within a node’s transmission range receive its transmission.

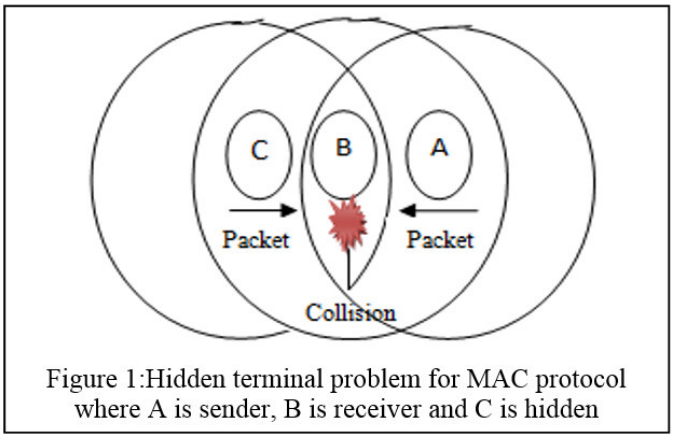

Figure 1:Hidden terminal problem for MAC protocol where A is sender, B is receiver and C is hidden

For example, in Fig. 1, node A is transmitting to node B. C is trying to communicate with node B simultaneously. According to the CSMA protocol, node C senses the medium, but since C is out of A’s transmission range, it fails to understand that A is transmitting to B and finds the medium free. As a result, C accesses the medium, causing collisions at B. This phenomenon is known as hidden terminal problem and C is called the hidden terminal.

2.2. Sensor S-MAC

In the year of 2002, sensor S-MAC is designed for the wireless sensor network which is a contention based MAC protocol with integrated low-duty-cycle operation & it is a modification of IEEE 802.11 protocol.

A. Working Principle of the Components of Sensor S-MAC:

Periodic listen & sleep:

In many sensor network applications, nodes are in an idle mode for a long time if no sensing event happens. At that moment, data rate is very low and it is not necessary to keep nodes listening all time. The main technique for reducing energy consumption in S-MAC is to make each node in the network follow a frame which is consisted with a complete listen and sleep cycle. Normally, the frame length is the same for all nodes in network. SMAC reduces the listen time by letting node go into periodic sleep mode. After sleeping period each node wakes up for listening to see if any other node wants to talk to it. For example, if a node sleeps for half second and listens for the other half, its duty cycle is reduced to 50%. So we can achieve close to 50% of energy savings. For fixing the duration of time, S-MAC provides a controllable parameter duty cycle, whose value is the ratio of the listen period to the frame length. Listen period also fixed by some physical and MAC layer parameters. The user can adjust the duty cycle value from 1% to 100% to control the length of sleep period. For maintaining periodic listen & sleep, initial schedule is established by – Choosing and Maintaining Schedules & Maintaining Synchronization.

a) Choosing and Maintaining Schedules:

For choosing and maintaining schedule, each node maintains a schedule table that stores the schedules of all its known neighbors. Before starting periodic listen and sleep each node needs to choose a schedule and exchange it with its neighboring nodes. Here, we have to know about two terms: synchronizer & follower.

For reducing control overhead, we prefer neighboring nodes are synchronized together. That is, during listening period one node follows another node's scheduling time of listening and during sleeping period one node follows another node's scheduling time of sleeping though not all neighboring nodes can synchronize together in a multi-hop network. For example, two neighbouring nodes 1 and 2 may have different schedules but they can synchronize with different nodes, 3 and 4, respectively, as shown in Figure 2. Here, if node 1 want to synchronize with node 3 then it must broadcasts it's schedule to node 3 for synchronization. Here, node 1 is called synchronizer. When nodes exchange their schedules by broadcasting it to all its immediate neighbours it must be ensured that all neighbouring nodes can talk to each other even if they have different schedules. As shown in Figure 2 if node 1 wants to talk to node 2, it just waits until node 2 is listening.

Figure 2:Neighbouring nodes 1 and 2 have different schedules. They synchronize with nodes 3 and 4 respectively.

If the node receives a schedule from a neighbour before choosing its own schedule, it follows that schedule by setting its schedule to be the same. We call such a node a follower.In the figure 2, if node 1 selects a scheduling time for him then node 3 must follow the scheduling time of node 1 and choose it's scheduling time to keep pace with the scheduling time of node 1. Here, node 3 is called follower.By using synchronizer and follower, nodes follow the below steps to choose their schedule and establish its schedule table.

b) Maintaining Synchronization:

The listen/sleep scheme requires maintaining synchronization among neighbouring nodes. Although the long listen time can tolerate fairly large clock drift, they still need to periodically update each other's schedules to prevent it. Long updating schedules can be accomplished by sending a short SYNC packet which includes the address of the sender i.e. identification number of sender and the time of its next sleep. Receivers will adjust their timers immediately after they receive the SYNC packet. A node will go to sleep when the timer fires. If multiple neighbours want to talk to a node, they need to contend for the medium when the node is listening. The contention mechanism is the same as that in IEEE 802.11 which is stated earlier, i.e., using RTS (Request To Send) and CTS (Clear To Send) packets. The node that first sends out the RTS packet wins the medium, and the receiver will reply with a CTS packet and sender can sends DATA to receiver. When a node encounters an RTS collision, it goes to sleep until the next active period and when a node sends out an RTS successfully, it does not go back to sleep until the transmitted DATA packet is acknowledged. In order for a node to receive both SYNC packets and data packets, we divide its listen interval into two parts. The first part is for receiving SYNC packets, and the second one is for DATA packets as shown in Figure 3. Each part is further divided into many time slots for senders to perform carrier sense. For example, if a senderwants to send a SYNC packet, it starts carrier sense when the receiver begins listening and randomly selects a time slot to finish its CS (carrier sense). If it has not detected any transmission by the end of the time slot, it wins the medium and starts sending its SYNC packet at that time. The same procedure is followed when sending data. In figure 3, frame format of SMAC is shown.

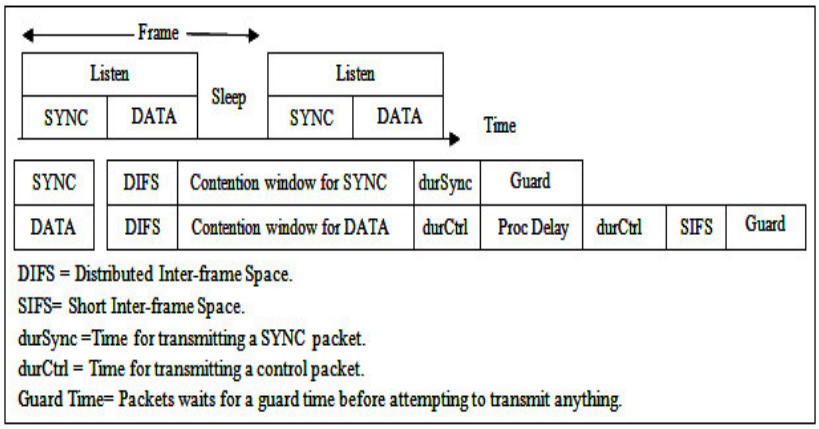

Figure 3: S-MAC frame format

Figure 4 shows the timing relationship of three possible situations that a sender transmits to a receiver. Here, two types of senders are shown. Sender 1 only sends a SYNC packet and sender 2 sends a SYNC packet and a RTS packet. In the case of sender 2 DATA is sent if only CTS is received. Each node periodically broadcasts SYNC packets to its neighbours even if it has no followers. This allows new nodes to join an existing neighbourhood. The new node follows the same procedure. At the receiver side, receiver sends CTS after getting RTS from sender. After getting DATA from sender, receiver sends ACK to sender. After getting ACK, sender goes to sleep mode. So, packets follow the sequences of RTS/CTS/DATA/ACK among sender and receiver for transmitting DATA.

Once transmission starts, it does not stop until completed. After the data transmission between nodes they simply follow a sleep schedule together. They do not follow their sleep schedules until they finish transmission. For this component, latency is increased due to the periodic sleep of each node and the delay can accumulate on each hop.

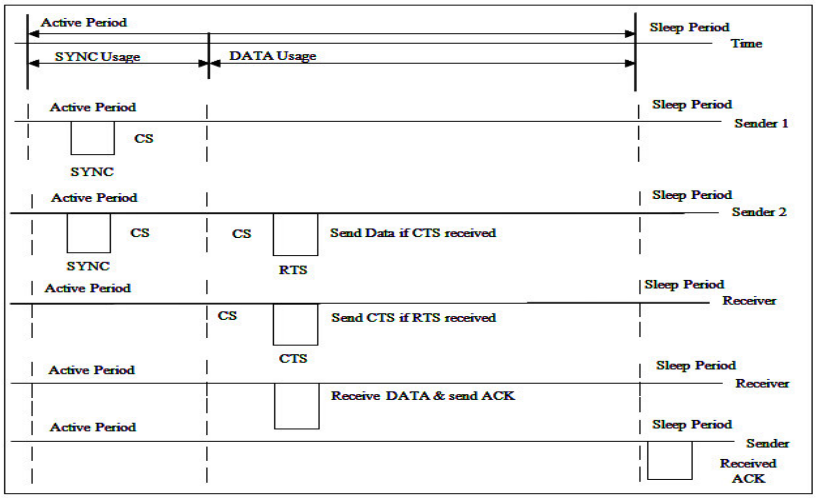

Figure 4: Timing relationship among a receiver and different senders. CS is carrier sense, ACK is Acknowledgement, RTS is Request to Send, CTS is Clear to Send & SYNC is synchronizing packets.

2)Collision and overhearing avoidance:

SMAC adopt the RTS/CTS mechanism to address the hidden terminal by adopting virtual carrier sensing for collision avoidance. In Virtual carrier sensing, there is a duration field in each transmitted packet that indicates how long the remaining transmission will be so that, if a node receives a packet destined to another node, it knows how long it has to keep silent. The node records this value in a variable called the network allocation vector (NAV) and sets a timer for it. When the NAV timer fires, the node decrements the NAV value until it reaches zero. If the value of NAV is not zero; a node determines that the medium is busy. So, the node doesn't send DATA to another. After carrier sensing before initiating a transmission, if a node fails to get the medium, it goes to sleep and wakes up when the receiver is free and listening again. Here, NAV is used to indicate the activity in its neighborhood. When a node receives a packet destined to other nodes, it updates its NAV by the duration field in the packet and a non-zero NAV value indicates that there is an active transmission in its neighborhood. The NAV value decrements every time when the NAV timer fires and a node can wake up when

its NAV becomes zero. In 802.11 each node keeps listening to all transmissions from their neighbor which is a significant waste of energy, especially when node density is high and traffic load is heavy. SMAC tries to avoid overhearing by letting interfering nodes go to sleep after they hear an RTS or CTS packet which prevents neighboring nodes from overhearing long DATA packets and the ACKs.

3)Message Passing

S-MAC adopts a modified fragmentation mechanism for transmitting a long message, called message passing. A *message* is the collection of meaningful, interrelated units of data which can be a long series of packets or short packets. Transmitting a long message as a single packet results high cost of re-transmitting the long packet if only a few bits have been corrupted in the first transmission. Moreover, if fragmentation of the long message into many independent small packets is made, we have to pay the penalty of large control overhead and longer delay. It is so because the RTS and CTS packets are used in contention for each independent packet in every transmission. Only one RTS packet and one CTS packet are used for a long message which is divided into many small fragments, and transmit them in burst. Every time a data fragment is transmitted, the sender waits for an ACK from the receiver. If it fails to receive the ACK, it will extend the reserved transmission time for one more fragment, and re-transmit the current fragment immediately. Switching the radio from sleep to active does not occur instantaneously. Therefore, it is desirable to reduce the frequency of switching modes. The message passing scheme tries to put nodes into sleep state as long as possible, and hence reduces switching overhead.

B. Some Limitations of Sensor S-MAC:

- Broadcast data packets do not use RTS/CTS, which increases collision probability.
- Adaptive listening incurs overhearing or idle listening if the packet is not destined to the listening node.
- Sleep and listen periods are predefined and constant, which decreases the efficiency of the algorithm under variable traffic load.
- SMAC scheduling mechanism works when self-configuration is in set mode. In the listen period, a node senses its neighbor nodes and transmits SYNC packets that contain randomly generated schedule. Thus a long time is taken by each node to get synchronized. For instance, if 10 nodes are implemented in the network, they have to wait 100 seconds to setup the schedule and for 15 nodes the time rises to 150 seconds. Thus a longer time for stabilization takes place in proportion to the number of nodes in a network [7].

2.3 Performances analysis and Simulation

Energy efficiency and throughput are two main performance metrics for designing power efficient MAC protocols.

1) Efficiency of energy savings:

The main source of sensor node is battery. It is seen that it is cost-effective to replace the nodes rather than changing or replacing them. Energy efficiency of the sensor nodes can be defined as-

Energy Efficiency = (Remaining energy) / (Initial energy) %

Efficiency of a protocol in transmitting the information through the network depends on the above ratio. If the value of this ratio is lass then the nodes give better performance. Energy efficiency can be increased by minimizing the energy wastage like: collision, overhearing, idle listening and packet overhead. IEEE 802.11 uses more than twice energy than SMAC while passing message from one node to another. As idle listening happens rarely, in this phase SMAC can't save energy much. Avoiding overhearing and efficiently transmitting long message save energy in SMAC. So, energy efficiency of SMAC is higher than IEEE 802.11. From Fig. 5, we can see that energy efficiency of SMAC increases with the increment of sensor nodes than IEEE 802.11. At a time energy efficiency rate of IEEE 802.11 become stable. So, we can say that SMAC is well-designed power efficient MAC protocol than IEEE 802.11.

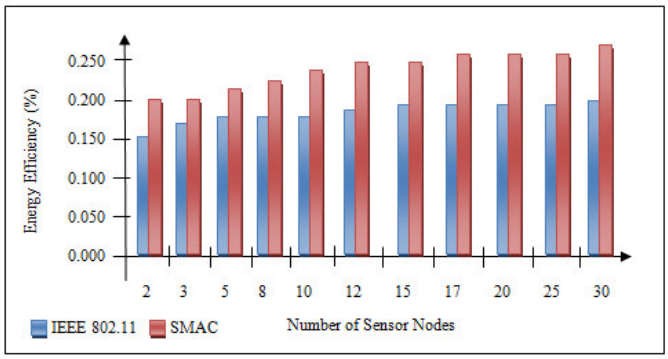

Figure 5: End-to-End energy efficiency of IEEE802.11 & SMAC for 30 nodes [8]

2)Network Throughput:

Network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps). Bandwidth measures the maximum throughput of a computer network. Better throughput of a network can be achieved if the sink nodes receive more data. Some sensor network applications sample the information with fine temporal resolution.

Network Throughput = Total bytes in data packets received / Timefrom first packet generated at source to last packet received at the sink node

Here, we find the throughput between the MAC protocols IEEE802.11 & SMAC & compare their outputs. We compute the throughout, using the payloads received at the MAC layer.

Experiment platform: Network Simulator version 2 (NS-2) has been used as experiment platform. NS-2 provides extensive support for queuing algorithms, routing protocols, multi-cast protocols and IP protocols over both wired network and wireless network.

Topology: We have simulated wireless sensor networks with regular topology as well as randomly generated topology.

Traffic pattern: We attach a UDP agent and a CBR traffic source to the sink node. The CBR source generates 20 packets (each 80 Bytes, because it will be added with 20 bytes IP header at the routing layer, so the actual size at MAC layer is 100 Bytes).

Routing Protocol: DSR, Simulation Time: 100 sec, Number of nodes: 20 and 40.

Simulation Parameters settings:

Some important parameters used in the steady-state simulations are listed in the Table 1.

TABLE 1

Default values of SMAC parameters	
Parameter name	***Value***
SMAC_DUTY_CYCLE	10%
SMAC_MAX_NUM_NEIGHBORS	20
SMAC_MAX_NUM_SCHEDULES	4
SYNCPERIOD	10s
SIZEOF_SMAC_DATAPKT	512 bytes
durDataPkt_	43ms
syncTime_	55.2ms
dataTime_	105ms
listenTime_	160.2ms
sleepTime_(10% duty cycle)	1442.8ms

New Now, we measure the performance i.e. throughput along with bandwidth vs. time by applying simulation on wireless sensor network with MAC protocols IEEE802.11 & SMAC.

2.4. Simulation Result

We know that, IEEE802.11 consumes much energy for idle listening, collision, overhearing and control overhead etc. In SMAC, these problems can be reduced by using ‘sleep periods’ and consumes less energy than IEEE802.11. Though S-MAC reduces energy consumption this saving may be offset by decreased throughput.

When we run simulation we see that, IEEE802.11 uses much bandwidth than SMAC but gives a higher

throughput. As SMAC uses sleep period (when data rate is very low and it is not necessary to keep nodes listening all the time) for which duty cycle is reduced to 50% & we can achieve close to 50% of energy savings. But during this period bandwidth utilization is very low. So, throughput is also low. Moreover, SMAC follows synchronization among nodes for avoiding collision. For this reason when a synchronizer starts transmission, it will not stop until finishing transmission. So, synchronizer occupies the bandwidth for it during transmission. As, few nodes take part in transmission, throughput becomes low.

In the figure 6(a), we run the simulation among 20 nodes for both IEEE802.11 & SMAC and we see that, when we use IEEE802.11, at a certain time all nodes start to sense the medium & when find that the medium is not busy they start transmission. For this, there was a higher use of bandwidth & we got a higher throughput though there may be packets loss, higher energy consumption is occurred.

When we use SMAC, at a certain time nodes start to sense the medium & when one node does not hear a schedule from another node, it randomly chooses a time to go to sleep and immediately broadcasts its schedule to its neighbouring nodes in a SYNC message which indicates that it (synchronizer) will go to sleep after a time, t seconds. Before that time it will transmit packets and occupies bandwidth. So, at this time only a few nodes (synchronizers) can utilize the bandwidth & give a lower throughput.

In the figure 6(b), we run the simulation among 40 nodes for both IEEE802.11 & SMAC and we see that, due to the less control overhead of SMAC there is higher throughput than IEEE 802.11 but with the advancement of time for increased sleep time distance between sender and receiver increases in SMAC and last received ACK packet will be in higher order so the drop of packet happens. So, after a certain time all packets drop in SMAC and we get no throughput.

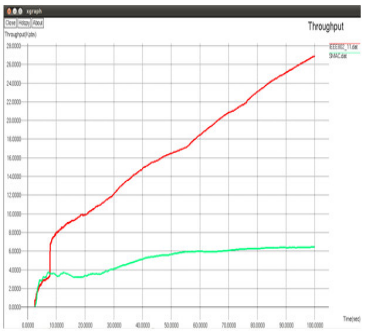

Figure 6(a): End-to-End throughput of IEEE802.11 & SMAC for 20 nodes

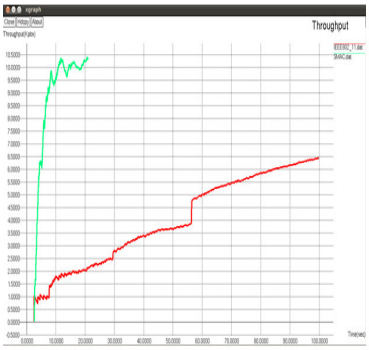

Figure 6(b): End-to-End throughput of IEEE802.11 & SMAC for 40 nodes

3.Conclusion

In the end we can say that, as a power saving protocol SMAC is very efficient than IEEE 802.11. It can remove idle listening problem, control packet overhead, hidden terminal problem but by using this protocol we get lower throughput than IEEE 802.11 if we increase the number of sensor nodes.

References

[1] Rajesh Yadav, Electronis and Radar Development Establishment Defense R & D Organization, Bangalore, India ; ShirshuVarma, Indian Institute of Information Technolgy, Allahabad, India; N. Malaviya, Institute of Engineering & Technology, Lucknow, India. A SURVEY OF MAC PROTOCOLS FOR WIRELESS SENSORNETWORKS. UbiCC Journal, Volume 4, Number 3, August 2009.

[2] IlkerDemirkol, CemErsoy, and FatihAlagöz; Bogazici University. MAC Protocols for Wireless Sensor Networks: A Survey. IEEE Communications Magazine • April 2006

[3] Chipcon Corporation. CC2500 Single Chip Low Cost Low Power RF Transceiver,Data Sheet. 2005.

[4] Woo and D. Culler. A Transmission Control Scheme for Media Access in Sensor Networks.In Proceedings of ACM Mobicom, Rome, Italy, July 2001.

[5] J. Polastre. A Unifying Link Abstraction for Wireless Sensor Networks.PhD thesis, University of California, Berkeley, October 2005.

[6] P. Ferrari, A. Flammini, D. Marioli, and A. Taroni, “IEEE802.11 sensor networking,” IEEE Transactions on Instrumentation and Measurement, vol. 55, no. 2, pp. 615–619, 2006.

[7] D Saha, M R Yousuf, and M A Matin. Energy efficient scheduling algorithm for s-mac protocol in wireless sensor network.

[8] Ioannis Mathioudakis, Neil M. White , Nick R. Harris , Geoff V. Merrett; Electronic Systems and Devices Group, School of ECS, University of Southampton, SO17 1BJ, UK. “Wireless Sensor Networks: A Case

Study for Energy Efficient Environmental Monitoring".
[9] Wei YE, John HEIDEMANN, Deborah ESTRIN; Information Science Institute, University of Southern California, Los Angeles, USA, Computer Science Department, University of California, Los Angeles, USA. An Energy-Efficient MAC Protocol for Wireless Sensor Networks. Published Online June 2008 in SciRes .

Authors

Bushra Rahman had received her B.Sc. in CSE from Military Institute of Science and Technology,Bangladesh in 2012. Recently, she is working as Lecturer in CSE Department, City University, Bangladesh.

Md. Rafiqul Islam had received his B.Sc. in CSE from City University,Bangladesh in 2013. Presently, he is working as Lecturer in CSE Department, City University, Bangladesh.