Performance analysis of CSMA and IEEE 802.11 in Wireless Sensor Networks using GloMoSim and IEEE 802.11as a gimmick

Shaiful Alam Chowdhury[†], **Mohammad Tauhidul Islam**[††]

[†]Stamford University Bangladesh, Dhaka, Bangladesh
[††]University of Lethbridge, Alberta, Canada T1K3M4

Abstract
Since its birth wireless communication became an indispensible part of the modern society. One major area that has a gigantic impact on the performance of wireless sensor networks (WSNs) is the Medium Access Control (MAC) layer. Many random access protocols exist in wireless sensor networks. Some of these protocols include Carrier Sense Multiple Access (CSMA), Multiple Access with Collision Avoidance (MACA), Multiple Access with Collision Avoidance for wireless (MACAW) and IEEE 802.11. All the protocols mentioned above except CSMA use Request To Send/Clear To Send (RTS/CTS) packets to avoid collisions (hidden terminal problem) which was a great problem for CSMA and that is the reason CSMA is almost obsolete for wireless communications. But after using RTS/CTS packets the protocols have to encounter some extra problems such as, energy consumption and end-to-end delay. The objective of this paper is to show the pros and cons of using RTS/CTS packets by comparing CSMA (does not use RTS/CTS) and IEEE 802.11 (uses RTS/CTS packets). We also portray that under some specific scenario the IEEE 802.11 is outperformed by CSMA which is also the novelty and contribution of this research work. This observation suggests that a lot of works have to be done to consider IEEE 802.11 an approximate perfect MAC layer protocol for WSNs.

Index Terms
CSMA, IEEE 802.11, MAC layer protocols, RTS/CTS.

I. Introduction

The ongoing progress in miniaturization, power-efficient wireless communication, micro sensor and microprocessor hardware, small-scale energy supplies in conjunction with the significant progress in distributed signal processing, ad hoc networks protocols and distributive computing have made Wireless Sensor Networks (WSNs) a novel technological vision [1][2]. As the Internet has revolutionized our life through the exchanges of diversified information readily among a large number of users, WSNs may very well, be equally significant by providing information regarding the physical phenomena of interest and ultimately being able to detect and control them or enable us to construct more exact models of physical worlds.

A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous gadgets using sensors to cooperatively monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [3][4].

The evolution of wireless sensor networks was originally motivated by military applications such as battlefield surveillance [5]. Remote sensors may help eradicate some of the confusions related to combat .They may be used to collect accurate information about on going battlefield conditions and providing apt information to the soldiers, vehicles and weapons in the battlefield [6]. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, vehicle detection and flare stack monitoring [3][7].

We can foretell a future where various persons with various types of medical conditions will be provided constant monitoring by the use of sensors which monitor physical situations. Perhaps for some kinds of medical conditions, remote sensors might be able to apply remedies [6].

The distribution of power will be managed better when the use of remote sensors will start. For example in 2001, although nimiety electricity existed in other states of the country, the Californians could not receive electricity. This situation can be avoided by monitoring the power load on the electrical line through the sensors[6].

Besides one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communication device, a small microcontroller, and an energy source, usually a battery. The size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust although functioning specks of genuine microscopic dimensions are yet to be designed [3]. The key features of a sensor node are its limitations in energy, transmission power, memory and computing power. So, the MAC layer protocols should be

Manuscript received October 5, 2010
Manuscript revised October 20, 2010

aware of the fact that, the memory of the nodes should not overflow and energy consumption at the nodes is minimized.

II. Related works

MAC stands for Media Access Control. A MAC layer protocol is the protocol that controls access to the physical transmission medium on a network [8]. It tries to ensure that no two nodes are interfering with each other's transmissions and deals with any possible interference. After the evaluation of diversified problems in Wireless Sensor Networks we can say that a perfect MAC layer protocol must have at least some properties to cope with the situations such as, handle hidden terminals, minimize energy consumption, successfully handle memory overflow problem and allow exposed terminals to talk.

In CSMA (Carrier Sense Multiple Access) a node willing to transmit first checks to see whether the transmission medium is free to transmit, if it is not the case then it waits for the medium to be free and then transmit at the next available time slot otherwise it starts transmitting right away [8]. The CSMA protocol has been used in a number of packet-radio networks [9][10]. Although they are trivial in nature and can achieve acceptable throughput under certain situations, they suffer from the well-known "hidden terminal" and "exposed terminal" problem in multi-hop wireless sensor networks, which significantly deteriorates their performance [11][8].

In Fig. 1 suppose node A is transmitting to node B and simultaneously node C is trying to communicate with node B. 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 [8].

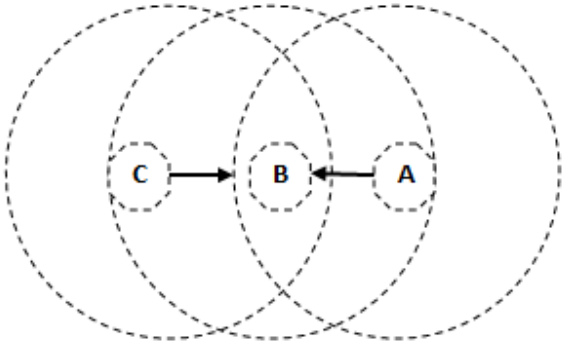

Figure-1: Hidden terminal problem for CSMA

In Fig. 2 suppose node A is transmitting to node B and after some time node C wants to transmit to D. According to the CSMA protocol, node C senses the medium, finds that node A is transmitting and waits (node C) until node A is finished with its transmission. This occurrence is known as exposed terminal problem which is responsible for degrading the network performance [8], because from the above scenario we find that node C could transmit to node D without collision and hence save a significant amount of time.

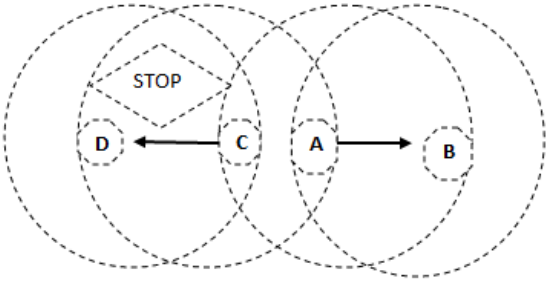

Figure-2: Exposed terminal problem

IEEE 802.11 adopted the technique of using RTS (Request to Send)/CTS (Clear to Send) to eliminate the "hidden terminal" problem [8]. In most of the situations this technique works fine but under certain circumstances the IEEE 802.11 fails to solve this "hidden terminal" problem which is shown in Fig. 3.

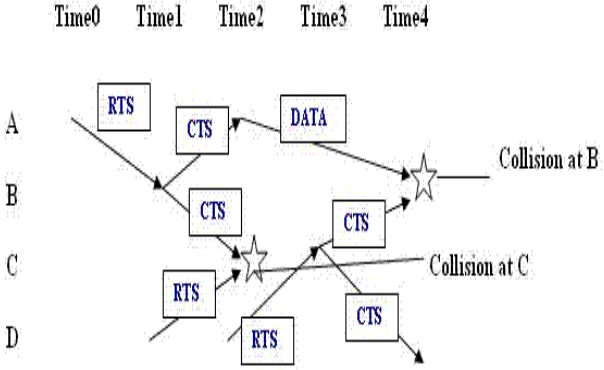

Figure-3: Hidden terminal problem after using RTS/CTS control packets

The scenario in Fig. 3 can be portrayed as; A wants to send data packet to B. So A sends RTS to B. Upon receiving the RTS, B sends CTS to A and C. At the same time D sends RTS to C for transmitting data packet. The CTS and RTS packets collide at C. After receiving CTS from B, A transmits data to B and D resends RTS to C. On this occasion C sends CTS to B and D. The data and CTS packets collide at B.

From the above mentioned sequence of events we find that the “hidden terminal” problem is not fully solved using the IEEE 802.11. The use of RTS/CTS control packets and ACK partially solves the hidden node problem but the exposed node problem remains unaddressed like CSMA [12], which is shown in Fig. 4.

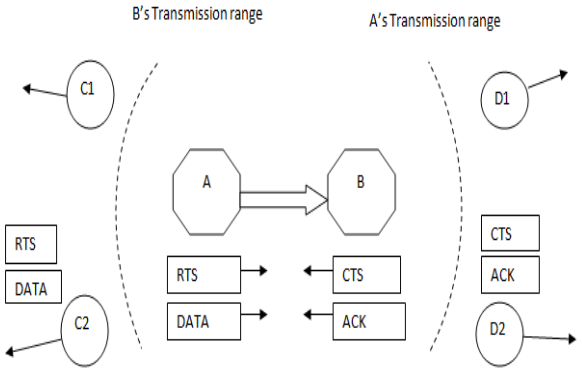

Figure-4: Exposed terminal problem for IEEE 802.11

From Fig. 4 we can see C1,C2 are exposed nodes when node A broadcasts RTS in order to transfer data to node B and D1,D2 are also exposed nodes when node B Broadcasts CTS in the response of RTS from node A.

Another problem that is associated with IEEE 802.11 but very rare with CSMA is the memory overflow problem at the nodes because of using extra RTS/CTS control packets. This is the reason for which the following happens with IEEE 802.11-until a saturation point is reached as the offered load increases the number of successfully received packets also increases whereas, after the saturation point the number of successfully received packets is reduced rapidly because of the limited memory of the nodes [13].

We already mentioned that the MAC layer protocols have great impact on the performance of wireless sensor networks. So a lot of works have been done for the improvement of MAC layer protocols. An important work described in [14], is current random access MAC protocols for ad hoc networks support reliable unicast but not reliable broadcast. So in this paper, they proposed a random access MAC protocol, Broadcast Support Multiple Access (BSMA), which improves broadcast reliability in ad hoc networks. In the paper [15] performance analysis between CSMA/CA that is carrier sense multiple access with collision avoidance and IEEE 802.11 is done which is closely related to our work. As the exposed node problem is not solved in IEEE 802.11, a solution for that problem is described in [12]. In the paper [16] a very important work has been done where they found the strength and weakness of different MAC layer protocols which will help to select a specific protocol for a specific work. Though RTS/CTS technique is responsible for some extra problems, as it plays a vital role for MAC layer protocols numerous works have been done to minimize the problems associated with using the RTS/CTS.

III. PERformance comparison using GloMoSim-2.03

To find out where it is not efficient to use IEEE 802.11 we evaluated and compared the performance of CSMA and IEEE 802.11 by setting the parameters to different values (for fewer number of nodes to higher number of nodes with fewer number of packets to higher number of packets). The performance metrics that we used for comparison are; percentage of packet loss, end-to-end delay, average throughput in the destination node and energy consumption.

The discarding of data packets of a node in a network because of its (node’s) limitation in speed at which it can process incoming data and a limited amount of memory in which to store incoming data is known as packet loss [17].

The time taken for a packet to be transmitted across a network from a source to a destination is known as end-to-end delay which includes queuing delay, processing delay, transmission delay and propagation delay [18].

The throughput is the measurement of how fast data can pass through an entity. In other words, if we consider this entity as a wall through which bits pass, throughput is the number of bits that can pass this wall in one second [17].

The energy consummated by the nodes in the network in order to communicate with each other is known as energy consumption.

We adopted for Global Mobile Information System Simulator (GloMoSim) for the simulation purpose because it is a widely accepted and scalable simulation environment for large wireless networks. GloMoSim uses a parallel discrete-event simulation capability provided by Parsec [15]. Here simulation time is set to 500 minutes and the Terrain dimension is set to 150 by 150 for 50 nodes. Then the dimension is changed for 100, 150, 200, 250 and 300 nodes. Node placement is uniform which means that based on the number of nodes in the simulation; the physical terrain is divided into a number of cells. Within each cell, a node is placed randomly. The default value of RADIO-TX-POWER was 15.0 and RADIO-RX-THRESHOLD was -81.0 but these are changed to 9.0 and -71.0 to set the transmission range of the nodes to approximately 100 meters. Five fixed sources are used to send data to node number 99 (destination for all the sources) when the number of nodes is 100. The destination is changed to node number 199 when the number of nodes in the network is 200 and similar changes for other number of nodes in the network. That is sources are always fixed but the only destination node is the last node (in number) in the network.

So as the number of nodes in the network is changed the destination node is also changed.
If the RADIO-TX-POWER is 15 dBm and RADIO-RX-THRESHOLD is -81 dBm then the transmission range is 668.57 meters which is the default value for GloMoSim-2.03. But for the convenience of our simulation purpose we tried to make the transmission range close to 100 meters. For that purpose we set RADIO-TX-POWER to 9 dBm and RADIO-RX-THRESHOLD is -71dBm. But even after that we could not get the transmission range exactly 100 meters. So, we took it as 99 meters.
To analyze, we collected the results from glomo.stat file and modified the code of GloMoSim developed by Parsec to get the result in an excel file. The graphs derived from the statistics found in glomo.stat file are given below:

A. Percentage of packet loss for 500 packets and 5000 packets

From Fig. 5(a), for CSMA the percentage of packet loss increased from 20% to near 80% with the number of nodes increased from 50 to 200. But after that the percentage of packet loss was almost constant. From Fig. 5(b), when the number of packets was 5000 then for CSMA the percentage of packet loss was 84% to near about 96%.

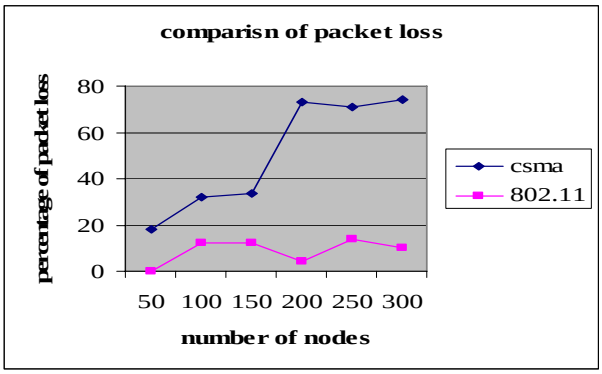

Figure-5(a): Percentage of packet loss for CSMA and IEEE 802.11 (500 packets)

For IEEE 802.11 and for 500 packets from Fig. 5(a), we see that the percentage of packet loss is very low. For 50 nodes the percentage of packet loss is approximately zero. It remains below 20% for the number of nodes from 50 to 300 which is very good. But from Fig. 5(b), for IEEE 802.11 and 5000 packets we see that the percentage of packet loss is very high. It started from above 80% for 100 nodes and it went to approximately 98% for 400 nodes. It is significant to note that, although IEEE 802.11 uses the RTS/CTS control packets to solve the hidden terminal problem and also uses acknowledgement for packet loss, packet loss remains a great problem in a high traffic network for IEEE 802.11. In our simulation we observed memory overflows at the nodes in high traffic network for IEEE 802.11. So for overflow problem there is no great difference between CSMA and IEEE 802.11 in case of reliability for a congested network.

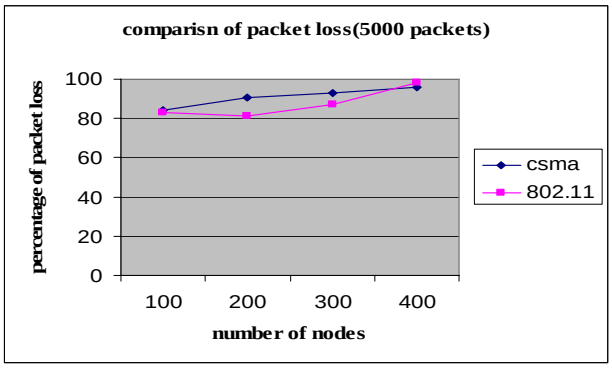

Figure-5(b): Percentage of packet loss for CSMA and IEEE 802.11(5000 packets)

B. Average End-to-End delay for 500 packets and 5000 packets

From Fig. 6(a) we find that, for CSMA the average end-to-end delay for 500 packets remains between 0 to 4 seconds which is very good. From Fig. 6(b) we observe that, for 5000 packets the average end-to-end delay remains between 0 to 4 seconds.

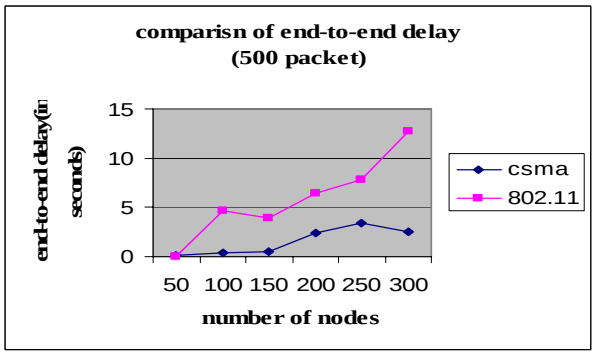

Figure-6(a): Average End-to-end delay for CSMA and IEEE 802.11(500 packets)

But from Fig. 6(a) we see that, for IEEE 802.11 the average end-to-end delay for 500 packets is clearly in increasing order and from 0 to near about 13 seconds. From Fig. 6(b), we also observe that the average end-to-end delay went high for IEEE 802.11 up to approximately 17 seconds when packet number was 5000 for 100 nodes to 300 nodes. But the surprising matter is that it falls down to 5 seconds for 400 nodes. The reason is that for 400 nodes most of the packets were lost due to the overflow problem.

The average end-to-end delay for IEEE 802.11 is generally more than CSMA because of the extra RTS/CTS control packets and as it tries to solve the hidden terminal problem by restricting a node to access the medium when one of its neighbors is transmitting. So in case of end-to-end delay CSMA is better than IEEE 802.11 most of the times.

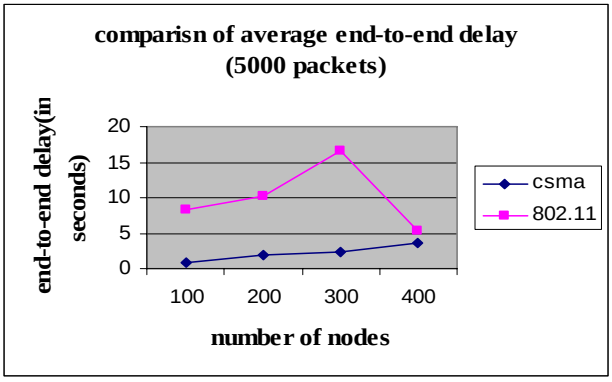

Figure-6(b): Average End-to-end delay for CSMA and IEEE 802.11(5000 packets)

C. Throughput for 500 packets and 5000 packets

From Fig. 7(a), for CSMA and for 500 packets we observe that the throughput is above 400000 bits per second when the number of nodes is 50. But for 100 nodes it falls down to approximately 75000 bits per second and when the number of nodes is between 150 and 300 the throughput always remains approximately 25000 bits per second.
From Fig. 7(b), for CSMA and for 5000 packets when the number of nodes is 100 the throughput is approximately 16000 bits per second but when the number of nodes is 200 it falls down drastically and it rises again at 300 nodes and again falls down to approximately 5 bits per second.

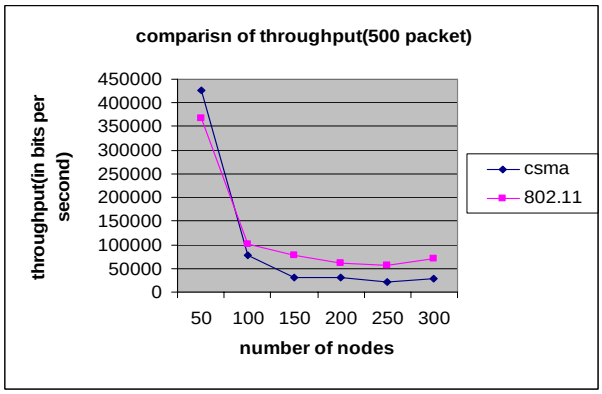

Figure-7(a): Throughput for CSMA and IEEE 802.11(500 packets)

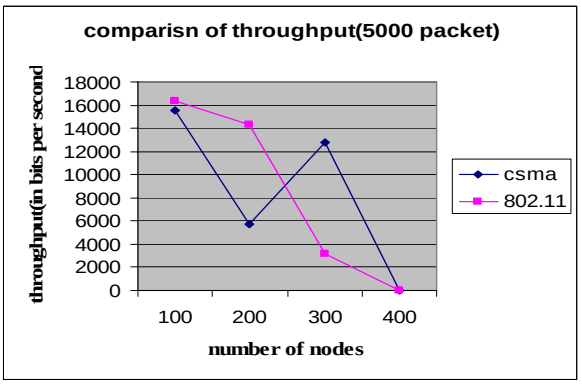

Figure-7(b): Throughput for CSMA and IEEE 802.11 (5000 packets)

We observe from Fig. 7(a) that, for IEEE 802.11 and 500 packets the throughput is above 350000 bits per second when the number of nodes is 50. But it falls down to 100000 bits per second when the number of nodes is 100 and it remains between 100000 and 50000 bits per second as the number of nodes goes to 300.
But from Fig. 7(b), for IEEE 802.11 and 5000 packets the throughput is unpredictable like CSMA in the same situation. So from our simulation we find that for high traffic network it is really unpredictable to decide which protocol is better in terms of throughput.
Throughput normally depends on the end-to-end delay and the packet loss and it is also expected that if the end-to-end delay is less and packet loss is small then the throughput will be good. From the simulation results for a low traffic network (for 500 packets) we find that the throughput for 802.11 is better than CSMA because the packet loss of CSMA is much worse than 802.11 though the end-to-end delay is less than 802.11. Because the advantage that CSMA gains over 802.11 by having less end-to-end delay is overwhelmed by the significant difference in packet loss with respect to 802.11.
But in case of congested network (for 5000 packets), the difference in end-to-end delay and the difference in packet loss in combination does not make any significant difference in the throughput for CSMA and 802.11. This is the reason behind the unpredictable results obtained for a congested network in case of throughput.
As mentioned earlier only the average throughput in the destination node is considered for this research work.

D. Energy Consumption for 500 packets and 5000 packets

From Fig. 8(a) and 8(b) we see that, IEEE 802.11 always consumed more energy than CSMA because of extra RTS/CTS control packets and possible retransmission. Whether a node is used in any data transfer process or not it has to consume some energy to remain alive in the network. Our calculation used the energy consumed by only those

nodes that were in the best path from source to destination excluding the energy consumed by the nodes to stay alive in the network. For achieving this we modified the radio_accnoise.pc file in which only the code inside the RadioAccnoiseFinalize method was changed.

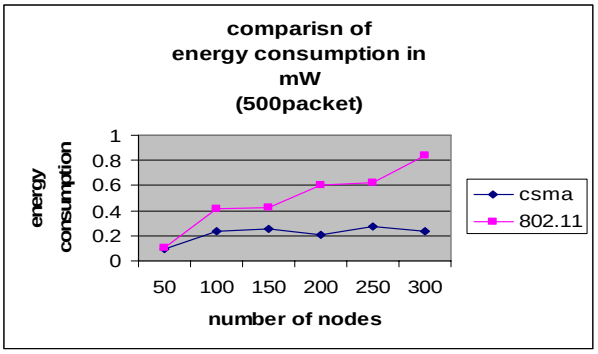

Figure-8(a): Energy consumption for CSMA and IEEE 802.11(5000 packets)

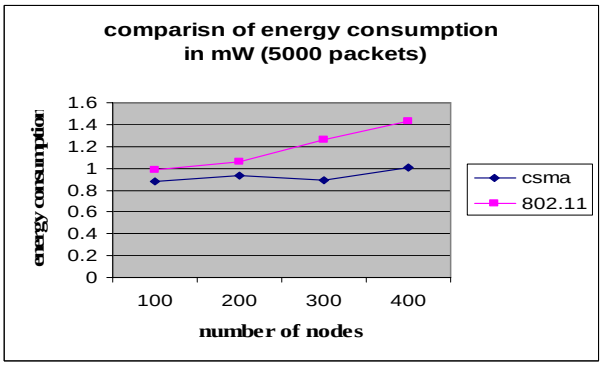

Figure-8(b): Energy consumption for CSMA and IEEE 802.11(500 Packets)

As the wireless sensor network is sensitive to the energy consumed by the sensors, in terms of energy consumption IEEE 802.11 is outperformed by CSMA.

IV. CONCLUSION

In this paper we find a lot of limitations for IEEE 802.11 as compared to CSMA though IEEE 802.11 is the standard MAC layer protocol. As IEEE 802.11 uses extra RTS/CTS control packets to solve hidden terminal problem it needs more energy and more time to transmit data than CSMA. Also it is not always better than CSMA in case of throughput. The only case when it is better than CSMA is in terms of percentage of packet loss for low traffic networks. But for high traffic networks it performs the same as CSMA for the memory overflow of the nodes or sensors.

It would be really tempting to solve the exposed terminal problem and the partially solved hidden terminal problem in IEEE 802.11. More analysis on the overflow problem could be performed to increase the average throughput and decrease the packet loss. Comparing the performance of CSMA and IEEE 802.11 with all the routing protocols to determine which routing protocol is best with which MAC layer protocol (CSMA and IEEE 802.11) in specific situations could be a potentially fruitful research area.

We did not consider a highly congested network consisting of more than 5000 packets and also the network size was relatively moderate-having at most 400 nodes. The only routing protocol that we used was AODV, other protocols like Bellmanford, DSR was not considered. In real life a sensor node can be destroyed or used up which we did not take into account in our simulation. In real life source node can always vary whereas in our simulation we always used some fixed nodes as sources. Mobility of the sensor nodes was totally avoided. The terrain dimension was set to some specific values without any significant reason which could be addressed for further analysis.

Experiments on real networks may be performed for generating a better idea about the actual scenario.

References

[1] D. Estrin, R. Govindan, J. Heidemann and S.Kumar “Next Century Challenges: Scalable Coordination in Sensor Networks,” Proc. of Mobocom’99, Seattle, Pages 263-270, August 1999.

[2] H. Karl and A. Willig. ”A short survey of wireless sensor networks.” TKN Technical Report TKN-03-018, Technical University Berlin, October 2003.

[3] K. Romer and F. Mattern,. “The Design Space of Wireless Sensor Networks”. IEEE Wireless Communications.11(6):54-61, December 2004.

[4] Thomas Haenselmann (2006-04-05), "Sensornetworks". GFDL Wireless Sensor network textbook, retrieved on 2006-08-29.

[5] Th. Arampatzis, J. Lygeros and S. Manesis, “A Survey of Applications of Wireless Sensors and Wireless Sensor Networks”, Mediterranean Conference on Control and Automation Limassol, Page 719-724, June 27-29, 2005.

[6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, Wireless Networks Journal (WINE), September 2002.

[7] S. Hadim and N. Mohamed , " Middleware Challenges and Approaches for Wireless Sensor Networks". IEEE Distributed Systems Online, 7(3), March 2006.

[8] “A Comprehensible GloMoSim Tutorial”, compilation by Jorge Nuevo, INRS - Universite du Que bec, March 4, 2004.

[9] L. Kleinrock and F. Tobagi, “Packet Switching in Radio Channels: Part I--Carrier Sense Multiple- Access Modes and Their Throughput-Delay Characteristics”, IEEE Transactions on Communications, 23(12):1400-1416, December 1975.

[10] R. L. Brewster and A. M. Glass, “Throughput Analysis of Non-Persistent and Slotted Non-Persistent CSMA/CA

Protocols," 4th International Conference on Land Mobile Radio, pp. 231-6, 1987.
[11] L. Kleinrock and F.Tobagi, "Packet switching in radio channels: Part II - the hidden terminal problem in carrier sense multipleaccess modes and the busy-tone solution", IEEE Transactions on Communications, 23(12): 1417-1433,1975.
[12] D. Shukla, L. Chandran-Wadia and S. Iyer, "Mitigating the Exposed Node Problem in IEEE 802.11 Ad Hoc Networks", 12th international conference on Computer Communications and Network, Pages 157-162, 2003.
[13] J. Liu, D. M. Nicol, L. F. Perrone and M. Liljenstam, "Towards High Performance Modeling Of The 802.11 Wireless Protocol", Proceedings of the 2001 Winter Simulation Conference, Pages 1315-1320, 2001.
[14] K. Tang and M. Gerla, "Random Access MAC for Efficient Broadcast Support in Ad Hoc Net- works", Wireless Communications and Networking Conference, volume-1, Page 454-459, 2000.
[15] T. Ho, K. Cben. "Performance Analysis of IEEE 802.11, CSMA/CA Medium Access Control Protocol",7thIEEE international Symposium on Personal, Indoor and Mobile Radio Communications, Volume-1, pages 407-411, 1996.
[16] I.Demirkol, C. Ersoy, and F. Alagöz, "MAC Protocols for Wireless Sensor Networks: A Survey", Communications Magazines IEEE, 44(4):115-121, 2006.
[17] Behrouz A. Forouzan, " Data Communications and Networking", Tata Mcgraw-Hill, 3rd edition, 2004.
[18] James F. Kurose, Keith W. Ross, "Computer Networking", Addison-Wesley, 5th Edition, 2009.

Shaiful Alam Chowdhury was born in Chittagong, Bangladesh on November 10, 1984. He is now a M.Sc. student in BUET (Bangladesh University of Engineering and Technology) and also a full time faculty of Stamford University Bangladesh. He received his B.Sc. in Computer Science and Engineering (April, 2009) from University of Chittagong, Bangladesh securing 1st position in the department. His current research interests are wireless sensor networks and algorithms.

Mohammad Tauhidul Islam is now a full time faculty in American International University-Bangladesh in the department of Computer Science. He obtained M.Sc. in Computer Science from University of Lethbridge, Alberta, Canada in 2009 and B.Sc. in CIT (Computer science and Information Technology) from IUT (Islamic University of Technology), Gazipur, Bangladesh in 2005. His research interest includes wireless sensor networks, security issues related to RFID and study and analysis of hard problems and possible approximation algorithms for those.