Hidden and Exposed Nodes in Wireless Sensor Networks

M.G. Kavitha and S. Sendhilnathan

1Assistant Professor-Department of CSE, University College of Engineering Pattukkottai, Rajamadam-614701 TamilNadu, India.
2Associate Professor-Department of Physics, University College of Engineering Pattukkottai, Rajamadam-614701 TamilNadu, India.

Received 28 February 2017; Accepted 22 May 2017; Available online 6 June 2017

ABSTRACT

Wireless Sensor Networks (WSNs) can be widely adopted to monitor the environment in agricultural, security and ecological applications. It is well-known that the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)-based wireless networks suffer seriously from the hidden terminal problem and the exposed terminal problem. In this paper, we present a joint solution to the two problems. Analysis and simulations show that the proposed scheme can significantly reduce the hidden and exposed terminal problems. Not only it can significantly improve the throughput of the network and the fairness among different flows, it can also provide a much more stable link layer.

KEYWORDS: CSMA/CA, Hidden terminal problem, Exposed terminal problem, WSNs.

INTRODUCTION

Wireless sensor networks have wide-range of applications, usually involve some kind of tracking, controlling or monitoring. Specifically these applications include healthcare applications, fire detection, traffic control, habitat monitoring, object tracking and nuclear reactor control. A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery. They also contain one or more sensing unit, and power unit.

In this paper we are trying to explore various aspects of medium access control (MAC) protocols in wireless sensor network. Creating a sensor network infrastructure, establishing communication links for data transfer between them and efficiently share communication resources between each sensor nodes are the important objectives of MAC protocol. Sensors nodes must need less amount of energy since they are small size devices they. A good sensor network must be fault tolerant, self-organizing and self-configuring, in case of some parts of nodes may fail, so designing such a MAC protocol for wireless sensor network is always an inspirational issue.
A Medium Access Protocol:

To enhance the lifetime of network, a good MAC protocol for the wireless sensor network must be energy efficient. A good quality of MAC protocol should gracefully contain such network changes. Although, there are various MAC protocols such as Time division multiple access (TDMA), carrier sense multiple access (CSMA), Frequency-division multiple access (FDMA), Wireless Sensor MAC (Wise MAC) and Code division multiple access (CDMA) which have already proposed for sensor networks, there is no protocol accepted as a standard [2] [3] [4] [5] and so designing a MAC protocol is always a challenging research space. MAC protocol is application-dependent, which means that there will not be one standard MAC for sensor networks. Lack of standardization at lower layers (physical layer) and the (physical) sensor hardware and energy preservation are the features of MAC protocol. The pattern of energy use in the sensor nodes depends on the nature of the application. As the applications of WSNs are large and diverse, the proposed protocols display much diversity.

To avoid co-channel interference among nearby cells, appropriate channel allocation schemes are required to allocate channels to both base stations and access points. If different nodes at same time trying to access the shared channel between them, they cause packet collusions and the packet might be lost. The most common MAC protocols for sensor network are based on CSMA scheme or different. In such scheme the transmitting node first senses the medium to check whether it is idle or busy [6]. The node is following its own transmissions to prevent collations with exiting signal if the medium is not free. To avoid packet collusions problem, another well know solution algorithm was IEEE 802.11.

Request-To-Send (RTS)/Clear-To-Send (CTS) exchange resulting in nodes getting exclusive access to the shared channel for a defined time period. However, the use of RTS/CTS-like schemes introduce again an unfair channel usage, where some nodes that heard the RTS/CTS exchange refrain from transmission even though they would not have interfered with ongoing transmission [exposed node problem]. Another problem which is unsolved by 802.11 RTS/CTS acknowledgement and handshake packets is hidden terminal problem. Hidden terminal problem is happened due to the two node stations that can’t hear the signal sense of each, if they are out of each one ranges. In such cases the interference is caused by the simultaneous transmission of two nodes [4].

MAC-deadlock, channel allocation problem, hidden and exposed terminals are happened in such shared channels. So the performance of wireless sensor network is directly affected with such problems. These problems cause throughput degradations and unnecessarily waste of channels between the nodes. Even though several works have been done to solve these problems, still they are not good enough to solve these problems.

B. Carrier Sense Multiple Access (Csma):

In Carrier Sense Multiple Access:

1. If the channel is idle then transmit.
2. If the channel for communication is free then it is going to transmit without any precaution that there might be collision.
3. If the channel is busy, wait for a random time.
4. Waiting time is calculated using Truncated Binary Exponential Backoff (BEB) algorithm.

![Carrier Sense Multiple Access](image)

**Fig. 1: Carrier Sense Multiple Access**

II. Problem Definition:

A. Hidden Terminal Problem:

Hidden terminal interference is caused by the simultaneous transmission of two node stations that cannot hear each other, but are both received by the same destination station [7]. Hidden nodes are the nodes that are not in the range of other nodes or a group of nodes. In a wireless network, it is possible that the node at the far edge of the access point’s range, known as r, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point’s range, r2. These nodes are known as hidden. The problem is when nodes r and r2 start to send packets simultaneously to the access point. Since node r and r2 cannot sense
the carrier, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) does not work. To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme.

Fig. II: Hidden terminal problem

The transmission range of access point A reaches at B, but not at access point C, similarly transmission range of access point C reaches B, but not at A. These nodes are known as hidden terminals. The problem occurs when nodes A and C start to send data packets simultaneously to the access point B. Because the access points A and C are out of range of each other and resultant they cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point B due to the hidden terminal problem.

The hidden terminal analogy is described as follows:
- Terminal A sends data to B, terminal C cannot hear A
- Terminal C wants to send data to B, terminal C senses a “free” medium (CS fails) and starts transmitting
- Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission to B
- Terminal A is “hidden” from C and vice versa.

Hidden terminal problem is solved using RTS/CTS. IEEE 802.11 uses 802.11 RTS/CTS acknowledgment and handshake techniques over wireless networks to transferring packets that partly overcome the hidden node problem. RTS/CTS are not a proper and permanent solution and may decrease throughput even further, but adaptive acknowledgments from the base station can help.

Some other technologies that can be employed to solve hidden node problem are:

*Increase Transmitting Power from the Nodes:*
With the enhancement of the transmission power of access point can solve the hidden terminal problem by allowing the cell around each node to increase in size, encompassing all of the other nodes.

*Use Omni directional antennas:*
Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks.

*Remove obstacles:*
Keep away the obstacles that affect the performance of access point accessibility.

*Move the node:*
Provide the mobility features to the nodes.

*Use protocol enhancement software:*
Pooling and token passing strategy should be used before start data transformation.

**B. Exposed Terminal Problem:**
In wireless networks, when a node is prevented from sending packets to other nodes because of a neighboring transmitter is known as the exposed node problem.
Consider the above specified wireless network having four nodes labeled A, B, C, and D, where the two receivers are out of range of each other, yet the two transmitters (B, C) in the middle are in range of each other. Here, if a transmission between A and B is taking place, node C is prevented from transmitting to D as it concludes after carrier sense that it will interfere with the transmission by its neighbor node B. However note that node D could still receive the transmission of C without interference because it is out of range from B. Therefore, implementing directional antenna at a physical layer in each node could reduce the probability of signal interference, because the signal is propagated in a narrow band.

The exposed terminal analogy is described as follows:

- B sends to A, C wants to send to another terminal D not A or B
- C senses the carrier and detects that the carrier is busy.
- C postpones its transmission until it detects the medium as being idle again
- But A is outside radio range of C, waiting is not necessary
- C is “exposed” to B

In the case of hidden terminal problem, unsuccessful transmissions result from collisions between transmissions originated by a node such as node A which cannot hear the ongoing transmissions to its corresponding node B. The probability of such a collision is proportional to the total number of terminals hidden from node A. In the case of exposed terminal, unsuccessful transmissions result from nodes such as node A being prevented from transmitting, because their corresponding node is unable to send CTS. Again such unsuccessful transmissions are proportional to the number of exposed terminals. Both these events lead to degradation of a node’s throughput. Hence it is observed that hidden terminals cause collisions, whereas exposed terminals cause unnecessary delay.

III. Related Work:

David Rodenas-Herraiz, Felipe Garcia-Sanchez, Antonio-Javier Garcia-Sanchez, Joan Garcia-Haro observed that there is no approach that reduces the HT and ET phenomena and simultaneously satisfies all the IEEE 802.15.5/ASES after performing a comparative evaluation of a group of significant proposals, showing which of them are the most suitable to be developed together with the ASES mechanism. Ketema Adere, Rammurthy proposed the directional antenna based MAC protocol that used with Sensor-MAC Protocol to increase the performance of the output of wireless sensor network. The directional antenna focusses energy in a particular direction, so that unfair channel allocation and wastage of channels between each node can be avoided.

L. Boroumand, R. H. Khokhar discuss the design factors of some existing mechanisms to deal with hidden node avoidance, and present a timeline of the development of these mechanisms. Abdelmalik Bachir and Dominique Barthel, Martin Heusse and Andrzej Duda propose a new access method for wireless multi hop sensor networks. It reduces collisions due to hidden nodes, a source of significant energy dissipation. Phan Van Vinh and Hoon Oh propose a reliable slotted broadcast protocol (RSBP) that allocates broadcast time slots to nodes based on their slot demands and then allows every node to transmit its broadcast message within the allocated slots.

IV. Proposed Approach:

In this paper we contributed a wireless sensor MAC protocol that effectively overcomes the MAC-deadlock, hidden and exposed terminal problem. A buffer available with common node performs it operation at the time when hidden nodes try to send data packets to it. All the data received by the buffer are scheduled for processing in common node using shortest job first scheduling algorithm which makes the waiting time to be genuine.

Before starting data transmission, the sender sends configuration message to all the reachable nodes indicating the destination node in the message. This configuration message which contains sender, receiver nodes identification handles problems that arise from exposed nodes.

V. Simulation Result

The problem of hidden and exposed terminal is a common problem in the shared medium access control of wireless network. Hidden terminal arises when two sender nodes out of range of each other transmit packets at the same time, to the same receiver, resulting in collisions at the receiver [1] [12]. Since sender nodes are out of
range of each other, they do not detect carrier even though the other node is sending data, and if their data packets reach the destination at the same time, these packets are dropped due to collision at the receiver. We have validated our solution using simulation. We consider energy consumption, location coverage, accuracy as measurement factors. The experiment region is a square area with the fixed size of 100 X 100 m² and the nodes were randomly placed. We deploy 100 sensor nodes in a two dimensional space. The simulation results are presented in the following figures.

Fig. IV: Random distribution of nodes

Consider the following cases when the hidden terminal problem could be happened in our simulations.

Case 1: When 2 nodes are in range of each other but they do carrier sense at the same time. In this case, since sender nodes do carrier sense at the same time, neither of the nodes is able to detect carrier, hence they both send data packets to the receiver at the same time, thus causing a collision at the receiver. Here we assume data packets reach the destination at the same time.

Case 2: When 2 nodes are out of range of each other and they do carrier sense at the same time. Here, since nodes are out of range of each other, they do not detect carrier, and their data packets reach the destination at the same distance, thus causing a collision and hence drop of packets. Here the data packets reached the destination at the same time that caused packets collusion.

Fig. V: Collision occurring at the destination. Loss of packets

Conclusion:

In this paper, at first, we have explained the hidden and exposed terminal problems in wireless sensor networks. These problems have an impact on the performance of throughput. We have briefly explained the solution methods. After analyzing the problems, we have proposed a Sensor-MAC Protocol to increase the performance of the output of wireless sensor network.

REFERENCES

4. Edgar, H. Callaway, Jr. —handbook of sensor networks: algorithms and architectures, the wireless sensor network MACI, chapter 8: 239.