Chapter 2

Literature Review

2.1 INTRODUCTION

In Cyber Physical Systems (Lee, 2008) accessing a channel holds a vital position, because change in medium access control method affects the performance of the whole networked system. Since this networked system is a combination of various wireless elements, the following related work focuses on those IEEE Medium Access Control (Ali et al., 2006) protocols which have been used to reduce as well as avoid collisions in Wireless Ad hoc Networks (Krishna and Iyengar, 2008) and Wireless Sensor Networks (WSNs) (Wu et al., 2011). This chapter also discusses the MAC protocol which is suitable for Cyber Physical Systems.

2.2 IEEE 802.11 MAC PROTOCOLS

It has been shown in many research papers that IEEE 802.11 MAC protocol (Krishna and Iyengar, 2008) performs an important task in wireless networking while accessing a channel. The MAC protocol with slot-reservation method helps the nodes to avoid collisions, when it tries to transmit any packet through a medium. This approach is a conventional Carrier Sense Medium Access-Collision Avoidance (CSMA/CA) (Krishna and Iyengar, 2008) method of 802.11 MAC protocol. Later various methods like Point Coordination Function (PCF) (Krishna and Iyengar, 2008) and the Distributed Coordination Function (DCF) (Krishna and Iyengar, 2008) were used to avoid collisions in a wireless communication while accessing medium.

As explained in (Krishna and Iyengar, 2008) the PCF has centralized medium access whereas DCF has medium access in a distributed manner. The latter approach uses a slotted and non-slotted process of binary exponential (Krishna and Iyengar, 2008) backoff methods. In these procedures the contention window is measured vigorously to lessen the collisions that occur during transmission of packets by nodes involved in it. This scenario is set only for wireless LAN networks.

The traditional procedure for decreasing the number of collisions which depend on backoff periods are enhanced by the Virtual Backoff Algorithm (VBA) mentioned in (Krishna et al., 2010). The authors of this paper have used the concept
of sequencing number technique (Krishna and Iyengar, 2008) in the VBA to reduce collisions by increasing the delay in the transmission. In (Krishna et al., 2010) VBA is applied with the two choices as Virtual Backoff Algorithm with Counter Sharing (VBA-CS) (Krishna et al., 2010) and Virtual Backoff Algorithm with Non Counter Sharing (VBA-NCS) (Krishna et al., 2010). Comparatively VBA-CS has tried to lessen the collisions that happen in each node’s backoff periods. Though the test results have shown that this procedure is better than previous approaches, it can only be applied for wireless networks of homogeneous type.

In the work of (Misra et al., 2013), the authors have revised the perception of VBA-CS to CPS kind of application through the learning automata model (Misra et al., 2013). It is known that in CPS environment the characteristics of each wireless network is different, and so the number of trials to access the channel is set according to the nature of a network involved in that application. The procedure had come up with improved results in terms of average delay and amount of loss percentage during packet transmission. In this methodology they have assumed that the nodes exhaust less energy by neglecting the bandwidth range of a node. This is especially done when a node from wireless sensor network needs to access a medium.

In (Misra and Khatua, 2014) it has been shown that successive collisions can be avoided in IEEE 802.11 protocol based wireless network using Semi-Distributed Backoff (SDB) (Misra and Khatua, 2014) approach. The process is carried out in two modes such as S-mode (sender) (Misra and Khatua, 2014) and R-mode (receiver) (Misra and Khatua, 2014). Initially a counter value is assigned to each node which ranges from 0 to number of nodes ready for transmission. A unique id (considered as signature) (Misra and Khatua, 2014) is assigned to each node at the sender. All these transmission packets are maintained in a buffer. When any of the (node’s) counter value becomes zero, the node transmits the packet after applying sender side backoff procedure.

At the receiver end using signature correlation (Misra and Khatua, 2014) method the signature id is checked from the transmission. If the number of signatures is more than one collision occurs, the communicated node packet is dropped and negative acknowledgement (NACK) (Misra and Khatua, 2014) is sent to corresponding sender node. Otherwise a node receives acknowledgement (ACK)
(Misra and Khatua, 2014) to denote the successful transmission. The SDB methodology used for Wireless Local Area Network (Misra and Khatua, 2014) assures channel accessibility. But at the subsequent stage when collision occurs, a packet is dropped rather than delaying the transmission.

2.3 IEEE 802.15.4 MAC PROTOCOL

The IEEE 802.15.4 standard (Lee et al., 2007; Xia et al., 2013) is a dynamic medium access control (Ali et al., 2006) protocol. This protocol provides two types of communications among the nodes in a sensor based networks. The structure of communication might be of star topological (Lee et al., 2007; Xia et al., 2013) way or point-to-point (Lee et al., 2007; Xia et al., 2013) communication. In a centralized structure the data transmission is one hop rather than multi-hop communication. The figure 2.1 depicts point-to-point communication and figure 2.2 shows the structure of centralized communication.

![Figure 2.1 Point-to-Point Communication](image)

In fully connected structure all the nodes communicate with each other and transfer the information among all the nodes. In IEEE 802.15.4 (Xia et al., 2013) the nodes that form a structure of point-to-point are called as Full Function Devices (FFDs) (Xia et al., 2013). All FFDs (Xia et al., 2013) should be in a reachable range of each other. In figure 2.2 the centre node is called as FFD (Xia et al., 2013) and the other nodes connected to it are called Reduced Function Devices (RFDs) (Xia et al., 2013).
et al., 2013). These RFDs (Xia et al., 2013) are considered as supporting devices which can perform simple processes with the help of FFD (Xia et al., 2013).

FFD (Xia et al., 2013) is treated as coordinator which connects all these supporting nodes and manages the whole wireless network. It also fetches the information frequently from these devices for upcoming process. FFD (Xia et al., 2013) acts as RFD (Xia et al., 2013) when it is sending information like device’s address to supporting nodes. In this wireless structure one RFD (Xia et al., 2013) cannot communicate with other RFD (Xia et al., 2013) in the same range; it can only disseminate the data through FFD (Xia et al., 2013).

Figure 2.2 Centralized Communication in CPS

All sensor with actuator based wireless networks use the centralized structure for data transmission. In this centre approach if any node joins the network or moves away from the existing network, an updation is made by the centre node which is also called as sink node (Xia et al., 2013). Since this centre node maintains the information about the network of limited range, it is also called as Personal Area Network (PAN) (Xia et al., 2013) coordinator.
The coordinator node (Xia et al., 2013) is responsible for sending the packets to the desired location by providing effective channel access (Ali et al., 2006). This protocol standard is applied in today’s smart networks like home automation, smart hospital, mechanisation of industry appliances, etc. All these new technologies use non-time based communication for transferring the data and receiving instructions correctly at an appropriate time.

2.3.1 MODES OF IEEE 802.15.4 PROTOCOL STANDARD

The IEEE 802.15.4 protocol (Xia et al., 2013) standard permits specific modes for transmission in any WSANs (Bragg et al., 2012; Xia et al., 2013). The two possible modes of wireless structure for transmissions are beacon-enabled (Xia et al., 2013) and non-beacon enabled (Xia et al., 2013).

a) The beacon-enabled mode (Xia et al., 2013) is also called as slotted mode (Xia et al., 2013). In this mode all the nodes communicate with the centre coordinator periodically to complete its transmission. This mode uses superframe structure (Xia et al., 2013) to synchronize with the centre coordinator.

b) The non-beacon enabled (Xia et al., 2013) mode is also referred as unslotted mode (Xia et al., 2013). In this mode devices need not wait for the centre coordinator to become free. As the data is generated the supporting devices transmit the data to the centre coordinator for further operation. Most of the smart wireless networks use this mode for data transmission nowadays.

2.3.2 SUPERFRAME STRUCTURE OF IEEE 802.15.4

The superframe structure (Xia et al., 2013) is applied only in the beacon-enabled (Xia et al., 2013) mode of IEEE 802.15.4 (Xia et al., 2013) protocol. This structure comprises three sections such as beacon (Xia et al., 2013), active (Xia et al., 2013) section and inactive (Xia et al., 2013) section. To initiate the process it is necessary to transmit two beacons initially. During the active (Xia et al., 2013) section the transmission takes place. The sensor devices save energy by changing to power off during inactive section.
Basically there are three parts in the active section of superframe (Xia et al., 2013) such as beacon (Xia et al., 2013), Contention Access Period (CAP) (Xia et al., 2013) and Contention Free Period (CFP) (Xia et al., 2013). Beacon start at the beginning followed by CAP (Xia et al., 2013) to complete the transmission. During this period the slotted method of channel access control (Ali et al., 2006) is applied. In the CFP (Xia et al., 2013) channel access control (Ali et al., 2006) procedure cannot be used. It exists till the end of the active section.

There are certain applications that require more time slots to complete the operation which hold special or critical data. To do so these devices have to request for additional slots to the centre coordinator. The slots allotted by centre coordinator are called as Guaranteed Time Slots(GTSs) (Xia et al., 2013). These slots are activated only on request to the centre coordinator. The centre coordinator checks for the availability of resources. If it exists, the requested node is permitted to continue its transmission.

The supporting devices using GTS (Xia et al., 2013) should complete its operation before the end of the CFP (Xia et al., 2013). Centre coordinator can assign maximum of seven GTSs in one superframe (Xia et al., 2013) structure. Though the number of GTSs (Xia et al., 2013) increases, the length of the active (Xia et al., 2013) section would not be increased. The length of the superframe structure and active period is calculated from the values of superframe order (Xia et al., 2013) and beacon order (Xia et al., 2013). When superframe order (Xia et al., 2013) value reaches its maximum limit the inactive period starts. The IEEE 802.15.4 protocol changes to non-beacon mode, when beacon order value reaches its maximum limit. In this mode superframe structure cannot be used.

2.3.3 SLOTTED CHANNEL ACCESS CONTROL METHOD

In IEEE 802.15.4 protocol the Carrier Sense Medium Access/ Collision Avoidance (CSMA/CA) (Xia et al., 2013) procedure is applied separately for slotted and unslotted mode. The choice of medium access procedure is dependent on the wireless structure setup. In both the modes transmission depends upon the backoff periods (Xia et al., 2013). In a time slot based mode, devices always coordinate with the time periods to complete its transmission.
As soon as the first time slot commences the transmission takes place. The data can be transmitted till the commencement of the next waiting slot. If device has not finished its transmission then it can continue its process in the next active period of superframe (Xia et al., 2013) structure. Similarly, all the devices in this wireless
structure complete transmission by letting other devices in operational and non-operational periods, alternatively.

The above figure 2.3 depicts the CSMA/CA (Xia et al., 2013) mechanism to be applied in the slotted mode of IEEE 802.15.4 (Xia et al., 2013) protocol to avoid collisions while accessing a channel.

In this methodology each device carries information about the number of attempts (NB), contention window size (CW) (Xia et al., 2013) and the waiting time (BE). Whenever a device starts its transmission number of attempts (NB) to access a channel is set to zero. And the following steps are performed.

Step 1: CW value is initialized to 2 to assess the channel accessibility. BE value is set as 3.

Step 2: Whenever the device senses that channel is busy it increases NB and BE value by 1.

Step 3: If BE has reached its maximum limit, to avoid more delay check if NB greater than 4, if so defers access to the device.

Step 4: if channel is idle, CW value is decremented by 1. This is to ensure that each device has to perform 2 Clear Channel Assessments (CCAs) (Xia et al., 2013) before any transmission.

Step 5: When CW becomes zero, the device is allowed to transmit the data till the commencement of next waiting period.

Step 6: If BE has not reached its maximum limit, then it has to repeat the process from step 1.

In the above methodology the device needs to wait for two CCAs (Xia et al., 2013) to access a channel. Moreover the waiting period should not be time-consuming so that the overall operation of the wireless system is ineffective. Considering all these issues, waiting period is set up to certain limit. Each time device initiates its transmission it has to calculate waiting time. For each retransmission, device needs to wait for another two CCAs (Xia et al., 2013).

Performing two CCAs (Xia et al., 2013) restricts the devices to access a channel at a time. Otherwise collision occurs when two or more devices approach a channel at the same time. In the slotted mode of channel accessibility the device need
not have to wait for any time slot. It will keep trying for channel access till it finds the medium to be free. In most of the sensor networks the slotted procedure is applied to avoid collisions while accessing a channel.

### 2.3.4 PRIORITY BASED IEEE 802.15.4 MAC PROTOCOLS

Cyber Physical System (Lee, 2006; Shi et al., 2011; Wu et al., 2011) is a developing research area which revolves around physical and cyber world. Various applications and performances of CPSs are discussed in (Lee, 2006; Shi et al., 2011; Wu et al., 2011). Most of the papers are focused on the collision avoidance in a wireless sensors network. Since CPS is based on Wireless Sensor Actuator Network (WSAN) (Bragg et al., 2012; Xia et al., 2013) in this section the CSMA/CA algorithms related to 802.15.4 protocol are discussed.

The authors of (Xia et al., 2013) had explained how CPS can be used in beacon-enabled and non-beacon enabled mode for avoiding collisions that occur while accessing a channel. This paper briefs about the superframe structure applied in beacon-enabled mode, and also discusses the traditional CSMA/CA (Xia et al., 2013) algorithm which applies Clear Channel Assessment (CCA) (Xia et al., 2013) with required back offs. In this approach contention window is used to delay the process of contending node when server is busy. Without contention window how the collision avoidance process can be carried out is also described in (Xia et al., 2013). But the conventional algorithm mentioned in (Xia et al., 2013) is not suitable for smart nodes.

In (Huang et al., 2008) the collision avoidance algorithm is based on Guaranteed Time Slots (GTSs) (Huang et al., 2008) which function on two levels. At the first level, all the devices are assigned with the priorities based on the GTS request from it. Devices requiring more GTSs are given top priorities. According to the adaptive methodology of GTS, which is called as Adaptive GTS Allocation (AGA) (Huang et al., 2008), the node’s packets are transmitted by the coordinator. This AGA algorithm executes in a beacon-enabled mode of IEEE 802.15.4 MAC protocol (Huang et al., 2008). At the next level nodes with lower priorities are considered if the server is idle. By giving more attention to top prioritized devices, they tried to solve the problem of node starvation. During critical situation, the coordinator would be busy with the data transmission of high priority node by letting the contending node
(holding important data) in a Contention Free Period (CFP) (Huang et al., 2008). So AGA fails to adapt to the emergency situation, occurs in the Contention Access Period (CAP) (Huang et al., 2008) of network.

Usually in a conventional 802.15.4 CSMA/CA algorithm two Clear Channel Assessments (CCAs) (Mounib et al., 2012) are used to check the status of a coordinator (busy or idle). But in (Mounib et al., 2012) the authors have showed that with more number of CCAs the level of collisions can be controlled up to certain extent during network communication. Based on the number of CCAs generated by a node, the coordinator allows accessing a channel. If a node encounters several back off periods, then that node will be given a chance to access the medium. The node put in the waiting period can start contention from its last CCAs, so that it can try for accessing channel in the forthcoming trials. In (Mounib et al., 2012) it has been proved that nodes contending for a channel recently will be given less priority than those which are contending for a longer time. This shows that the channel allocation by the coordinator is not fair for all the contending nodes in that network by neglecting precarious state that occurs.

The authors of (Na and Yang, 2009) focused on the sensitive applications based on data rate which operate in a non-beacon enabled mode of 802.15.4 MAC protocol. In this paper they have introduced separate virtual MACs that comprised two types of collision avoidance algorithms such as Adaptive Backoff Window Control (ABWC) (Na and Yang, 2009) and Virtual Collision Avoidance (VCA) (Na and Yang, 2009). The ABWC vigorously regulates the backoff window according to data rate in the local collision region of network. The VCA mechanism avoids the withdrawal of data rate transmission in a virtual collision region of network. These two approaches emphasis more on data rate constraint broadcasting and generating collision free packet transmissions virtually. But at certain level packets are blocked to avoid more collision which is a drawback of this approach.

In (Lu et al., 2013) the authors proposed a mechanism to utilize the channel efficiently based on priority in Wireless Sensor Networks (Lu et al., 2013). In this priority based CSMA/CA algorithm the sensor nodes are categorized into three types such as priority with level 0, 1 and 2 according to type of data and node capacity. After two consecutive Clear Channel Assessments (Lu et al., 2013), a node with priority 0 gets medium access by the coordinator. The nodes with priority 1 and 2 are set in a Contention Free Period (Lu et al., 2013) and its Contention Window is
decreased by 1. This is to handle data type of multimedia sent from the nodes. So this approach gives preference to top prioritized data to enhance the functioning of the network by consuming less energy. But most critical data handling is given less priority which decreases the performance of the wireless network.

In (Liu and Czylwik, 2014) the authors have shown how collisions can be reduced by implementing Adaptive Priority-Based (APB) (Liu and Czylwik, 2014) Service-differentiation CSMA/CA (Liu and Czylwik, 2014). This mechanism comprised two approaches such as adaptive backoff approach and priority-based service-differentiation algorithm. In the former method, node chooses appropriate backoff period based on the status of the channel. In the latter approach each node is assigned with backoff exponent value ($P_{BE}$) (Liu and Czylwik, 2014) and contention window length ($L_{CW}$) (Liu and Czylwik, 2014). A node with less $P_{BE}$ and $L_{CW}$ is treated as top priority node as it holds most important data. Thus this procedure allows for accessing a channel to these nodes (high priority) immediately. As a result when channel is busy, a large value is set as backoff period to reduce collisions in a network. When low prioritized node is contending for a channel and the high priority node is ready for transmission, the former node packet is blocked though it holds critical data. This degrades the performance of the network.

2.3.5 IEEE 802.15.4 MAC PROTOCOLS FOR WSAN

Medium Access Control (Ali et al., 2006) is a mechanism which provides a way for the portable devices to access a channel without any collision in a wireless structure. When a medium is to be shared among several portable devices, there is a possibility of an occurrence of traffic congestion. Due to this most of the node’s packets are dropped either on the way or from the server to which it is connected. As the scale of collision in any wireless network increases the performance of the network gets decreased. To overcome the issue of collision occurrence in any wireless network, several channel access (Ali et al., 2006) control mechanisms are implemented. These channel access (Ali et al., 2006) control mechanisms used the IEEE 802.11 protocol (Choi et al., 2005) group standards like 802.11/a/g/n (Choi et al., 2005; Lee et al., 2007) and IEEE 802.15 (Lee et al., 2007) standards like 802.15.4 or 802.15.6 (Lee et al., 2007).
Since today’s world is revolving around Internet technologies, an effective channel access (Ali et al., 2006) mechanism has to be introduced to avoid collisions. Moreover new technologies are built with sensor devices as well as sensor cum actuator based devices. These smart devices assist the people to perform any task in an easy and a rapid way in association with the Internet. When any transmission has to be carried out from one part of the globe to the other part, the sensor with actuator built devices play a major role in it. In this type of wireless communication Cyber Physical System (Lee, 2009) take a lead by executing relevant tasks at an appropriate time.

To provide channel access to several smart devices at time, CPS (Lee, 2009) uses IEEE 802.15.4 MAC protocol (Lee et al., 2007; Xia et al., 2013). Though this channel access control (Ali et al., 2006) protocol is mainly used for wireless sensor networks (WSNs) (Lee et al., 2007; Wu et al., 2011), it is effectively applied in wireless sensor actuator networks (WSANs) (Bragg et al., 2012; Xia et al., 2013). From the research study it is said that WSANs (Xia et al., 2013) are an extension of WSNs (Lee et al., 2007; Wu et al., 2011). This sensor with actuator based wireless network is suitable for executing CPS (Lee, 2009) based applications. In these wireless networks sensors collect the data and send it for further process to be completed. But in WSNs (Lee et al., 2007; Wu et al., 2011) sensor devices collect the information but will not disseminate the data for further action.

IEEE 802.15.4 standard (Lee et al., 2007; Xia et al., 2013) is considered as a less cost with short data bit range protocol which consumes less power during transmission. So this protocol standard is widely used as a transmission protocol for wireless networks which comprises of sensor cum actuator built devices. In (Xia et al., 2013) it is discussed that during data transmission the above said protocol acts as a link between the wireless structure devices and the Internet server. Because of this significant factor, in most of the CPS (Lee, 2009) based applications IEEE 802.15.4 protocol (Lee et al., 2007; Xia et al., 2013) is strongly recommended for channel access (Ali et al., 2006) and handover of data.

In the paper (Sayuti et al., 2014) a case study is done on Smart Home and Ambient Assisted Living (SHAAL) (Sayuti et al., 2014) system. In this system they use health and home related sensors to gather and process the data according to the
instruction received. The system is managed in such a way that a buffer is maintained to execute the information according to priority. High priority is assigned to health related data and low priority is assigned to other sensed data. The buffer acts like First Come First Served (FCFS) (Sayuti et al., 2014) queue.

The system is tested in two set ups such as centralized and de-centralized with the help of IEEE 802.15.4 protocol (Sayuti et al., 2014). Though the system functions in two different configurations, it will forward the high prioritized data first and then the low priority data (the smart home data). When any unpredictable situation rises the SHAAL system (Sayuti et al., 2014) fails to handle or manage such occurrence.

The authors of (Bragg et al., 2012) have proposed a two-level network for data transmission in Hospital Wireless Networks (Bragg et al., 2012). In the first stage the data is collected from Body Area Networks (BANs) (Bragg et al., 2012) connected with the patients. The data collected from the patients are placed in a queue maintained at Patient Data Controller (PDC) (Bragg et al., 2012). The PDC processes the data according to priority and transmit the information to the headquarters based on criticality. By using Reinforcement-Learning (RL) (Bragg et al., 2012) Queue Management technique, the instructions are delivered to the concerned doctors or staff heads in the hospital. In this approach they use multiple queues to monitor the patient’s conditions (high priority to low). Besides, the authors have tried to arrange and schedule the critical information from PDC to the headquarters using game theoretical method. Though the system focuses on prioritized data, it does not consider all system parameters to give importance to critical data.

In addition to the above literature study, in (Kortuem et al., 2010; Xia et al., 2012) the authors discussed how Internet has changed the lives of human in present day. The authors have specified that Internet of Things (IoT) (Atzori et al., 2010) had made the way easier for the hardware devices to combine with computational devices to perform certain activities like gathering the information, scheduling the events, estimating the arrival and departure time of automobile vehicles. Moreover this new technological approach assists the people in remote or inaccessible locations by providing necessary instructions. These instructions help them to get medical care free of cost.
The authors of (Wan et al., 2013) have explained how devices connect with other devices to enable reliable communication while transferring useful information. This is practically possible only if these devices are connected through integrated databases. These databases fetch the information from the sensor coordinators that are located in different regions but are connected with the Internet. Internet enriched applications become a part of CPS to manage the overall maintenance of the wide area wireless system in which human intervention is very less.

2.4 SUMMARY

This chapter discusses the various approaches that have been made to avoid as well as to reduce collision using sequencing technique based virtual backoff algorithm in IEEE 802.11 MAC protocol. Two variants of IEEE 802.15.4 channel access control procedures are discussed and explained how the channel access control procedure is applied in slotted mode of 802.15.4 protocol standard. It has been shown that how IEEE 802.15.4 MAC protocol can be used in both time-slot mode and unslotted mode for cyber physical system based network. In IEEE 802.15.4 collision avoidance is ensured based on top prioritized data rather than most critical data. Further it has been discussed that most of the approaches prevent collision in slotted mode of 802.15.4 MAC protocol. Besides those the study says that how succession collisions had been reduced effectively in 802.11 MAC protocol. Above all it is discussed that the Internet based applications maintain a large wireless structure application which is connected with an integrated database.