University of Stavanger

Term Project
DAT610_1 - Wireless Communications

# MAC Protocols in Nuclear Power Plants

*Junaid Alam [j.alam@stud.uis.no]*
*Ramprasad Beerappa [r.beerappa@stud.uis.no]*
*Bilal Amjad [b.amjad@stud.uis.no]*

Master of Science in Computer Science
Dept of Electrical Engineering & Computer Science
Faculty of Science & Technology

Autumn 2017

November 16, 2017

# Contents

**Abstract**

In this paper, we will study the requirements for a wireless sensor network to be deployed in a Nuclear Power Plant to detect the leakage and to monitor nuclear radiation. After the Fukishima Daiichi nuclear disaster that was triggered by a tsunami in 2011, many people in different countries are showing their concerns for the safety of the environment and for the closer of Nuclear power plants. However, as the natural resources like coal, fossil fuels and water are getting depleted, nuclear energy remains the major sources of energy to meet the demand and hence it is un-avoidable. To fully prevent or at least giving advance warning to the society about unforeseen disaster at a Nuclear Power Plant (NPP), utmost measures must be taken. Wireless Sensor Networks (WSNs) are widely getting popularity due to their easy to deploy and efficiency for constant monitoring of the environment.

**Keywords -** MAC protocols, Ad Hoc wireless networks, Nuclear Reactors, Mission Critical, Wireless Sensor Network, Nuclear Power Plant, Nuclear Radiation, Sensor MAC protocols.

# 1 Introduction

## 1.1 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are widely used in many applications nowadays to monitor particular activity within an area of interest. The rapid advances in hardware and the widely available wireless technologies have enabled to develop low power, low cost and more efficient sensor nodes. Usually in the wireless sensor networks, thousands of nodes are deployed in a close proximity and it is expected that the nodes can move independently. Since there exists no central or predefined infrastructure, the network must adapt to frequent change of topology. The type of networks where there is no fixed infrastructure are called Ad-hoc, which is a Latin word meaning "for this" [1]. In an ad-hoc network, new nodes can freely join or current node can leave the network without effecting other nodes.

However, since the sensor nodes come with limited power, utilization of the power is very important for a durable monitoring. In this paper, our main focus will be on choosing a MAC protocol for efficiently transmitting sensory data to a collecting node.

## 1.2 Nuclear Power Plant

The Nuclear Power Plants (NPP)[2, 3] is a thermal station that generates the electricity power using the heat energy generated by the nuclear reactors. The usual process to generate the heat energy is by nuclear fission. The generated heat energy heats the reactor coolant such as water or gas which in turn produces steam. The steam is fed into the turbines which finally generates the required electric power. The NPP environment falls into mission critical operations as the fuel used is very hazardous and hence requires careful operations of the NPP facility.

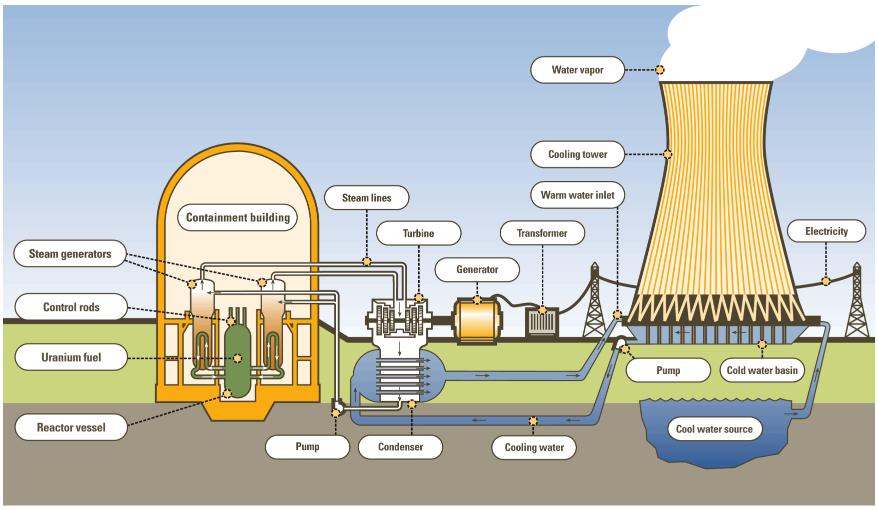



Figure 1: Nuclear Power Plant

In general the important components of a NPP are:

1. Generator
2. Containment structure containing nuclear reactors
3. Condenser
4. Cooling system
5. Safety valves
6. Feed water pump
7. Emergency power supply
8. Turbines

Some of the challenges in NPP operations of NPP are - Facility temperature, pressure, and humidity to avoid such as core meltdown, prevent radiations, plant reliability, prevent equipment failures, and reduce operational and maintenance costs. Also, the primary concern is with the accidents and incidents such as with radiations and loss of coolant accidents (LOCA).

Hence, the use of wireless sensor network will address the above challenges and operational concerns by providing efficient monitoring capabilities. For this, a wireless backbone network should be available in the facility. However, there are several concerns within itself to deploy the wireless sensor networks in the nuclear power plants such as electromagnetic and radio frequency interferences (EMI/RFI), security issues, installation issues such as coverage of the wireless signal, integration with existing data networks, signal propagation and footprint, and energy sources for the power to operate sensors, possible effect of wireless signals on the plant equipment, reliability issues such as bit/packet error rate (BER/PER) of the signals and their ratio for average error in bits. In addition, the challenge is to transmit data through containment with walls constructed with a line of carbon steel, reinforced concrete, and to deal with the equipment such as steam generators, crane structure, coolant pumps, pressuriser, etc.

The applications of wireless sensor networks can be used efficiently to monitor plant reliability, prevent equipment failure, reduce operational and maintenance costs, and prevent radiations.

Although there are some challenges in adopting wireless sensor networks in nuclear power plants, the resolutions that addresses those concerns can be achieved by redundancy of the sensor networks to prevent mishaps and also deployed as a backup network to the existing wired network which results in cost-effective without compromising safety.

Wireless sensor networks provide tremendous advantages in nuclear power plants such as redundancy in communication networks, less space of usage due to no additional or less wiring, robust and decent solutions for increased data recovery, online monitoring of critical components, reducing plant operation and maintenance costs, prevents forced outages, performance evaluation of the components, diversified monitoring capabilities, healthy environment for staffs, easy to extend or replace facilities, efficient access to information in remote areas, and enable mobile computing.

# 2 Medium Access Control Protocols

Sensor nodes sense the data from the environment and modulate their information over some carrier signal and finally transmit it back to the collecting node [4]. Since several nodes listen and transmit the data on a shared channel, there could be collisions. A collision occurs when two nodes transmit data at the same time using the shared channel. Media Access Control (MAC) protocols has been developed to reduce the collision using different techniques. Sine WSNs do not have a fixed infrastructure, the MAC protocols for WSNs should accomplish two requirements. Firstly, the sensor nodes have to form an ad-hoc wireless network to transmit data to a collecting node. Secondly, the protocol must give fair chance to all nodes to use the shared channel and transmit data efficiently. MAC protocols for sharing a channel can be divided into two groups: scheduled based protocols and contention based protocols [4].

In a schedule based protocols, the transmission medium is divided in to sub-channels either by time, frequency or orthogonal codes and assign the sub-channels to different nodes. Since different nodes use different sub-channels for transmission, the nodes in these protocols usually do not interfere with each other and are largely collision free. Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA) are schedule based MAC protocols that are widely used in wireless communication.

In a contention based MAC protocol, the nodes compete with each other for a shared channel. Sine many nodes compete for the same shared channel, collision occur in such systems. The example of contention based protocols are ALOHA and Carrier Sense Multiple Access (CSMA) protocols. In CSMA, a node senses the channel before transmitting. If the channel is busy, it retreats and retries later.

## 2.1 Carrier Sense Multiple Access

Carrier Sense Multiple Access (CSMA) is a contention based protocol that allocates the channel on demand. In this protocol, if the node has data to transmit, it senses the medium first. If the medium is free, it immediately transmits the data otherwise it waits and senses the medium again. There are different versions of CSMA including 1 persistent, p-persistent CSMA.

CSMA itself is straightforward and easy to implement protocol that requires no scheduling or fixed infrastructure. However, it is prone to some of the major problem in wireless medium access. The major obstacle is hidden terminal and exposed terminal problem.

Hidden terminal as depicted in Figure 1 occurs when node A hears node B but not C, and node C hears node B but not A. While node A is transmitting data to node B and node C also want to send data to node B. When node C senses the medium, it thinks the channel is idle and start transmitting. Since both node A and C are transmitting to B, the data is clearly going to collide at B due to the fact that node A is hidden to node C.

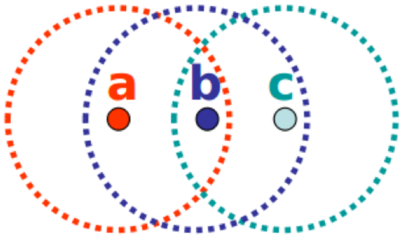



Figure 2: Hidden terminal problem

On the other hand, exposed terminal problem is caused by overhearing as shown in Figure 2. When node B is sending data to node A and node C want to send data to node D. When node C senses the medium, it thinks that the medium is busy so it retreats from transmitting. Hidden terminal caused data collision while exposed terminal utilize the shared channel poorly. To overcome the hidden terminal problem, CSMA-CA is developed. In CSMA-CA, nodes start a RTS-CTS handshake before transmitting data.

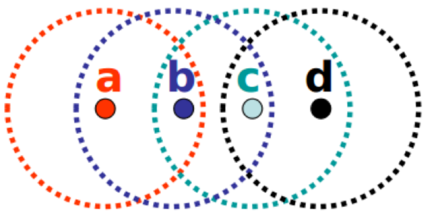



Figure 3: Exposed terminal

## 2.2 Time Division Multiple Access

Time Division Multiple Access (TDMA) is a schedule based protocol that allocates time slot to each node to access the channel one at a time. If there are N number of nodes in the network, each node is allocated a specific time slot. The total number of slots make up the frame as shown in Figure 3.

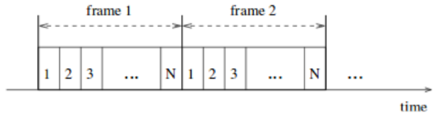



Figure 4: Time slot allocation in TDMA

In TDMA, the whole available bandwidth is used by a single node in its allocated time slot.

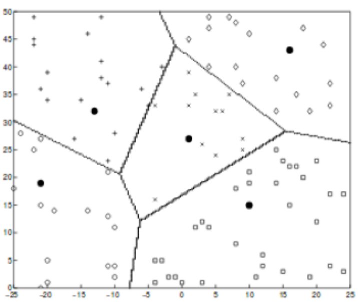
# 3 MAC Protocol for Wireless Sensor Networks

Although most of the MAC protocols designed for wireless communication are well tested, without modification they are not suitable for WSNs as WSNs differ from traditional wireless communication network such as cellular communication. The major difference in WSNs and traditional wireless network is that most of the sensor nodes are energy constrained and are usually deployed in environment where human reach is minimal, and recharging the batteries are usually not possible. Another difference is that the traditional wireless network has a well-defined network, however sensor nodes are often deployed in ad-hoc fashion where the nodes have to organize themselves and form the network [5].

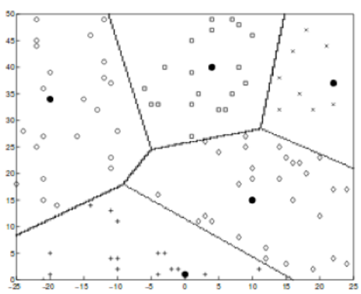
Schedule based protocol especially TDMA draws a lot of attention for sensor network. In TDMA, since the nodes only access the channel on its allocated time slot, the node can power off the radio component to save power. However, TDMA is not well adapted to frequent changes of network topology and it requires a strict time synchronization among nodes. Since contention based protocols does not need time synchronization and knowledge of network infrastructure, more researches are focused on contention based protocols.

**Low-energy adaptive clustering hierarchy**

Low-Energy Adaptive Clustering Hierarchy (LEACH) is hierarchical clustering protocol in which sensors organize themselves into cluster. In each cluster one node act as a cluster head while all non-cluster head nodes transmit their data to the cluster head. The cluster head receives data from all non-cluster head node and performs data aggregation before sending the data to the collecting node or base station BS [6]. Since cluster head has to receive data from all non-cluster head nodes and perform signal processing, this node is much more energy intensive than other nodes. Thus, LEACH protocols incorporate a randomized rotation of cluster head selection to avoid draining the battery of sensors in the network. Figure 4 shows the formation of cluster and cluster heads at time t1 and t2.



(a) Time T1



(b) Time T2

Figure 5: Cluster nodes at different time intervals

The operation of LEACH is dived into round. In each round, there are two phases, a setup stat and a steady state phase. Cluster heads are elected during the setup state and data are transmitted in steady state phase as shown in Figure 5.

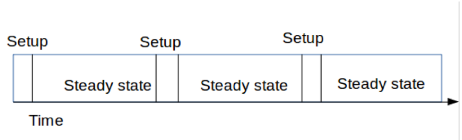



Figure 6: Operation phases of LEACH

At setup phase, each node independently decides whether or not to become cluster head at round r with threshold:

$$T(n) = \begin{cases} \frac{P}{1-P\,(r\,mod\,1/P)} & if\ n \in G, \\ 0 & otherwise \end{cases}$$

Where $P$ is the desired percentage of cluster heads in the network, $r$ is the current round number, and $G$ is a set of nodes that have not been cluster heads in last $1/p$ round [7].

A node randomly picks a number between 0 and 1 and compare the number with $T(n)$. If the number is number is less than $T(n)$, then the node become cluster head for this round otherwise the node become common node [8].

When the nodes have elected themselves to be cluster heads for the current round, they broadcast ADV message using CSMA MAC protocol. All non-cluster heads nodes send a Join-REQ message to cluster node to join based on signal strength received during ADV broadcast. To avoid hidden terminal problem, the transmission power is set so that all nodes can hear. Once the cluster head received Join-REQ from all joining sensors, it creates a TDMA schedule for the non-cluster nodes so that they can transmit data to cluster head on their allocated time slot [4].

To avoid intra-cluster collision, each cluster uses a different CDMA codes. To transmit data to collecting node, each cluster head node uses a dedicated CDMA code.

During the steady state, each non-cluster nodes transmit message to cluster head using the CDMA code allocated for its cluster. Since steady state uses TDMA for data transmission, nodes in a cluster turn their radio on only during their allocated time slot. By turning off radio, nodes avoid overhearing and greatly reduce collision and save power.

Since most of the sensor nodes in a cluster are located within short distance, the data they send to cluster head will be identical or redundant. When the cluster head receives data from all non-cluster nodes, cluster heads filters out the redundant data and send the aggregated data to collecting node. By data aggregation, cluster heads reduce the size of data to be transmitted to collecting node.

In LEACH protocol, cluster heads are selected by distributed algorithm. Instead of using distributed algorithm for cluster head selection, a centralized algorithm can be used to select cluster heads. LEACH-C is a protocol that uses a centralized clustering algorithm and the same steady state phase as normal LEACH.

In LEACH-C, collecting node selects the cluster heads based on the distance and energy of the nodes in the network. During the setup phase, all nodes send their location and energy information to collecting node. Collecting node compute the average node energy and nodes having lower energy cannot be cluster heads. Collecting node finds the cluster using annealing algorithm. Once collecting node computes cluster heads and their associated clusters, the collecting node broadcast a message that contains cluster head ID for each node. If a nodes ID and the cluster heads ID in the message matched, the node become cluster head otherwise the node become a non-cluster node and determines its TDMA slot for the data transmission. A non-cluster head node goes to sleep and wake up only in its allocated time slot to transmit data [6].

# 4 Experimentation

We have simulated [9] the LEACH protocol in MATLAB with a base station, randomized **100** nodes, **1000** rounds, cluster hierarchy model in a **100** $\times$ **100** yard. The base station is positioned at the centre of the of the yard. The default power/energy measured in joules is **0.5** and **5e-5** joules is utilized for transmitting, receiving each bit, data aggregation and compression. The cluster is created using the LEACH cluster algorithm with the default probability set to **0.05**. The control packet length is of **200** and data packet length is **6400**. For each round we are creating new cluster and compute the dissipated energy at the cluster head and non-cluster heads. Also, we compute either the node is alive or dead based on the available power/energy level at corresponding nodes. The captured data at each round is cached and the relevant plots are generated.

## 4.1 Wireless Sensor Network Topology

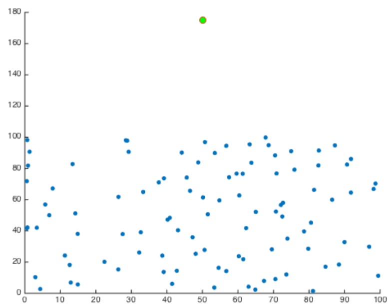



Figure 7: Randomly distributed nodes

The Figure-7 provides the wireless sensor network visualization with **100** nodes in a **100** yard and the base station.

### 4.2 Performance

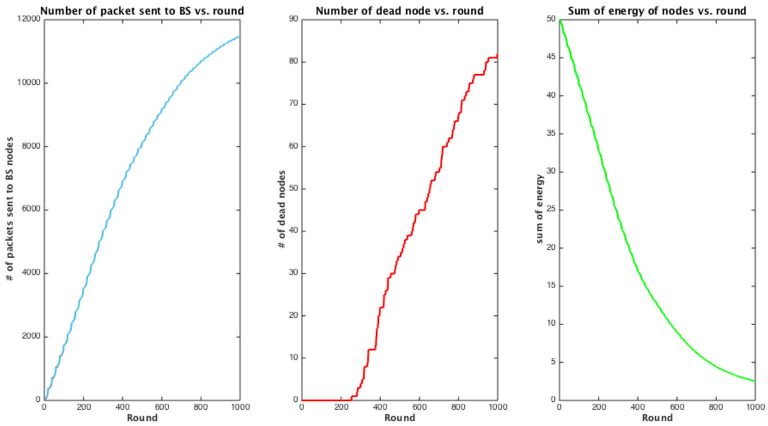



Figure 8: Network lifetime and energy consumption

The Figure-8 showcases two different interpretation of the captured data during simulation - Network lifetime against the rounds in the first two plots and the power at the nodes against the rounds in the third plot. In the first plot, we can visualize that as and when the number of rounds increases the number of packets sent to base station node also increases. But, after around 800 rounds, we see that the number of packets sent to base station slowly arrives to a saturation level. The second plot provides us the liveness of the nodes against the number of rounds. Initially, all the nodes are alive as there are less number of packets been transmitted. As and when the number of rounds increases, the total transmitted packet count since the beginning and due to the processing of phases in LEACH protocol over a period of time creates more dissipation of power at the nodes and hence the power at the nodes comes to NIL. Hence, the number of dead nodes increases. The third plot provides visualization of power at the nodes against the number of rounds over a period of time. As and when the number of rounds increases the number of packets transmitted and processing of phases in LEACH protocol increases. Hence, the power at the nodes drop.

# 5 Conclusion

Nuclear Radiation detection and monitoring is a measure needs to be taken without error. The advancement of wireless technologies make it possible to develop highly efficient sensors for detecting radiation wavelengths. However, a proper MAC protocol is needed for the sensors for prolong functioning. LEECH protocol is a low energy, self adapting protocols that can be used in a Nuclear Reactor. Our experiments shows that sensor nodes last longer and energy is prepositionally dissipated among all nodes.

# Bibliography


[1] http://www.learnersdictionary.com/qa/what-does-ad-hoc-mean

[2] H.M. Hashemian. *WHAT YOU NEED TO KNOW ABOUT SENSOR RELIABILITY BEFORE AND AFTER AND ACCIDENT*. IAEA TWG NPPIC Meeting, Vienna, Austria.

[3] Jeong-Kweon Lee*, See-Chae Jeong, Ki-Hoon Jeong, Do-Young Oh, Jae-Hack Kim. *Wireless Technology Application to Nuclear Power Plants*. McMaster University, 2005.

[4] N. Merizzi. *Sensor Network Deployment in the MacMaster Nuclear Reactor*. McMaster University, 2005.

[5] Wei Ye, John Heidemann. *Medium Access Protocol in Wireless Sensor Networks*. McMaster University, 2005.

[6] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan. *An application-specific protocol architecture for wireless microsensor networks*. IEEE Transactions on Wireless Communications, 2002.

[7] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan. *Energy-efficient communication protocol for wireless microsensor networks*. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2002.

[8] Chunyao FU, Zhifang JIANG , Wei WEI and Ang WEI. *An Energy Balanced Algorithm of LEACH Protocol in WSN*. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[9] Mohammad Hossein Homaei. *A Famous Clustering Routing Protocol in Wireless Sensor Networks*. https://www.mathworks.com/matlabcentral/fileexchange/.