Performance analysis of MAC based Flooding Protocol for Wireless Sensor Networks

Prof. Mrs. Urmila A. Patil
Associate Professor, DYPIET, Pune University

Ms. Smita V. Modi
Student, DYPIET, Pune University

Ms. Suma B. J.
Student, DYPIET, Pune University

Abstract

A Wireless Sensor Network (WSN) is a collection of thousands of tiny sensor nodes having the capability of wireless communication, limited computation and sensing. Wireless sensor networks (WSNs) are appealing to researchers due to their wide range of application potential in areas such as target detection and tracking, environmental monitoring, industrial process monitoring, and tactical systems. In this paper, all the components of a sensor node are discussed in brief. Also, Energy Consumption in Wireless sensor networks is one of the main challenges for researchers. Many researches have been done for extending the overall network lifetime by minimizing the power consumption of sensor nodes. Most of the work is done over the MAC layer of network in which different kinds of MAC protocol used by sensor networks. Most commonly used standard is 802.11. Here new approach is presented to enhance the performance of sensor node in terms of power consumption for both transmitter and receiver in the WSN. We propose standard 802.11 MAC layer protocol and flooding as a routing protocol. We are supporting the performance of proposed approach efficient through our extensive simulation work using the NS2. We will first implement the 802.11 MAC protocol and then do the cross layer simulation using Flooding routing protocol with different kinds of WSN networks and hardware evaluate its energy consumption performances. We have measured the performances in terms of total energy consumption, residual energy and average energy consumption.

Keywords- Wireless sensor networks, medium access control (MAC), flooding, NS-2.

I. Introduction

Over the past few years we have seen a tremendous growth in wireless-based networks and systems that has made the wide-spread commercial use of wireless devices - cell phone, global positioning systems (GPS), and pagers - possible. The rapid advancement made in the industry since the advent of wireless-based technology has led some research-based studies to believe and predict that wireless access in laptops, personal digital assistants (PDAs), mobile phones would overshoot wired access by later next year [Figure 1]. Furthermore recent advances in processor, memory and radio technology coupled with the advancement in the wireless technology has allowed portable devices to support several important wireless applications, including real-time multimedia communication, medical applications, surveillance using sensor networks.

Sensor network is a developing domain with operational demands unlike any other recent paradigm in wireless communication. Every functional specification of wireless sensor networks requires it to be different from the current wireless technology – sensor node densities being extraordinarily high, very low data rates, extremely low transmission and reception powers at the nodes, micro-sized nodes with expected sensor node lifetimes between 5-10 years on battery power. However, amidst the afore-mentioned specifics for the revolutionary wireless domain of wireless sensor networks lies the challenge of designing a system that can optimally incorporate all the functional specifications. While cheaper silicon and circuit complexity has allowed the realization of Moore's law allowing Integrated Circuits (ICs) complexity to double consistently over 18 months at an almost constant cost, Moore's law just seems inapplicable to apply to batteries. Depending on the particular chemistry of batteries and prolonged refinement of their constituents, energy densities of batteries has only doubled roughly over a time span of 5-20 years. The tremendous potential for rapid deployment of such networks is thus offset by their limited power reserves attributed to their minute size.

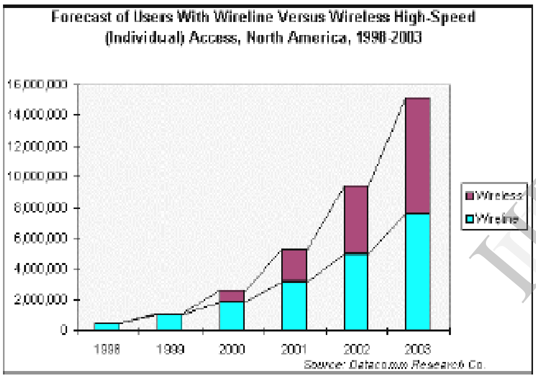

Figure 1. Predicting the usage of wireless access in comparison to wired access.

A. Wireless Sensor Networks

Wireless Sensor Networks (WSNs) represent a new paradigm in wireless technology drawing significant research attention from diverse fields of engineering. WSN technology is stated to be one of the "10 Emerging technologies that will change the world". The tremendous potential for rapid deployment of such networks is underway with busy researchers creating and optimizing WSN technology all around the world. The vision of many researchers is to create sensor-rich "smart environments" through planned or ad-hoc deployment of thousands of sensors, each with a short-range wireless communications channel, and capable of detecting ambient conditions such as temperature,movement, sound, light, or the presence of certain objects.

WSNs can be deployed extensively in the physical world and spread throughout our environment. They can be sited far from the actual occurrence and can still be used for data aggregation and collection from a remote location far away from the phenomenon. The WSNs comprise of a large number of application-specific wireless sensor nodes (typically in hundreds of thousands in number) spread over varying topographies. This kind of random placement of the sensor nodes does not follow any fixed pattern and the density of nodes is not dependent on any factor. Once they are deployed in the environment (under scrutiny where sensing needs to take place), these hundreds and thousands of nodes have to organize themselves in the network by listening to one another. They self-organize themselves by creating multi-hop wireless paths through mutual co-operation. The nodes work collectively and collaborate together on common tasks of sensing/data-collection/communications etc. to provide good network-wide performance in terms of network life-time, latency, and uniform density of available nodes for sensing.

WSNs offer unique benefits and versatility with respect to low-power and low-cost rapid deployment for many applications that do not need human supervision. Some of these applications include disaster recovery, military surveillance, health administration, environmental & habitat monitoring, target-tracking etc. Due to the large numbers of nodes involved in the WSN deployment new benefits to the afore-mentioned sensing applications including:

• Extended range of sensing - WSNs enable large numbers of nodes to be physically separated; while nodes located close to each other will have correlated data (e.g., these nodes will be collecting data about the same event), nodes that are farther apart will be able to extract information about different events.

• Robustness and fault-tolerance - Ensuring that several nodes are located close to each other and hence having correlated data makes these systems much more robust in terms of data sensing (even though it involves redundancy). In case of WSNs even if a small number of sensor nodes from a network fail, there is enough redundancy in the data from different nodes that the system may still produce acceptable quality information.

• Improved accuracy - While an individual sensor's data might be less accurate than another independent sensor's data (both sensor nodes are assumed to be in close proximity to the detected event) in the WSN, combining the data from nodes increases the accuracy of the sensed data. Since nodes located close to each other are gathering information about the same event, aggregating their data enhances the common signal and reduces the uncorrelated noise as well.

• Lower cost - Due to reduced size, reliability, and accuracy constraints on sensor nodes, these nodes are much cheaper than their high-accuracy high-complexity sensor counterparts.

However to be able to realize all the discussed specifications we need to design protocols that can provide appropriate support and allow the wide-spread use of WSNs.

Sensors are small nodes which are capable of data processing and communication. The sensor node measures ambient conditions from environment, transform it into electrical signals and sends via radio transceiver to a sink and then this aggregated information is sent back to a base station through a gateway [1]. Sensor networks are distributed sensors to monitor conditions like temperature, sound, vibration, pressure and pollutants etc. WSN links physical world and digital data network and provide a distributed network having the constraint of scalability, lifetime and energy efficiency.

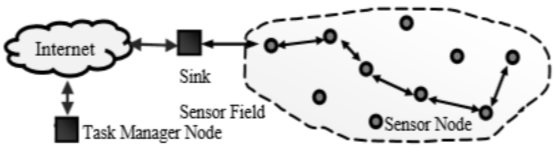

Figure 2. A Wireless Sensor Network

System Architecture and Design Issues Since routing protocols are application specific so the Performance of routing protocol is dependent upon the system architecture. The following issues are generally encountered [2]:

• Network Dynamics: Since the sensed event can be either static or dynamic so the most challenging task is to route the message among the nodes. Route stabilitybecomes an important optimization factor, in addition to energy and bandwidth.

• Node Deployment: The performance of the routing protocol is application dependent and it can be either deterministic or randomized.

• Data Aggregation: The elimination of duplicate data collected from different sensors is called data aggregation. Every node should have the capability of data aggregation because computation is less energy consuming than communication.

• Node Capability: A sink is more powerful than normal sensors in terms of energy and bandwidth. Some application requires cluster-heads with normal sensors for computation or aggregation.

• Data Delivery: The aggregated data through the sensors is delivered to the sink; this delivery can be continuous, query driven or hybrid. • Direct Vs Multi-hop: When all the nodes are close to the sink, direct routing is preferred. Since the transmission power is proportional to the square of the distance covered by data so in that case multi-hop routing is preferable.

II. Standard MAC 802.11 Protocol

A MAC protocol provides slightly different functionality depending on the network, device capability, and upper layer requirements, but several functions exist in most MAC protocols. In general, a MAC protocol provides [3]:

• Framing – Define the frame format and perform data encapsulation and decapsulation for communication between devices.

• Medium Access – Control which devices participate in communication at any time. Medium access becomes a main function of wireless MAC protocols since broadcasts easily cause data corruption through collisions.

• Reliability – Ensure successful transmission between devices. Most commonly accomplished through acknowledgement (ACK) messages and re-transmissions when necessary.

• Flow Control – Prevent frame loss through overloaded recipient buffers.

• Error Control – Use error detection or error correction codes to control the amount of errors present in frames delivered to upper layers.

Several aspects of sensor networks differentiate the MAC protocol design from MAC protocols in other networks. First, sensor nodes conserve energy by turning off unneeded hardware because most hardware, even when not active, consumes a non-negligible amount of energy. Thus, each sensor node must somehow coordinate with its neighbor to ensure both devices remain active and participate in communication. Sensor network MAC protocols most often performor actively participate inthis functionality so upper layers have only an abstract concept of viable links or topology information. Several techniques, such as schedule-based clustering and separate wakeup communication, exist and we mention them when used in the discussed protocols. Secondly, sensor networks produce traffic that differs from the communication patterns existing in other networks. Environmental monitoring provides a typical sensor network application. Sensor nodes monitoring a particular environmental characteristic periodically send data to a central entity for collection and analysis. These devices individually produce traffic at periodic rates with small payloads. Both the data characteristics, which may exhibit strong periodic generation and high spatial correlation, and the small payload size, which increases the impact of protocol overhead, differentiate sensor net- works from other networks. Third, the limited resources available to a sensor node prevent the use of common MAC protocol techniques. Many wireless MAC protocols constantly listen to the wireless channel for activity either for reception or before transmitting. However, a transceiver that constantly senses the channel will quickly deplete the sensor node energy resources and shorten the network lifetime to unacceptable levels.

Due to the popularity of the IEEE 802.11 [3] standard in wireless local area networks, we provide a brief introduction, but show that it does not suit sensor network applications for several reasons. IEEE 802.11 provides two modes of operation for wireless devices: an infrastructure mode where devices communicate through a central entity called an access point (AP) using the point coordination function (PCF), and an ad-hoc mode where devices communicate with each other directly using the distributed coordination function (DCF). The PCF extends upon the DCF and provides mechanisms for collision-free transmissions and device synchronization with the AP. Both the PCF and DCF use a channel access mechanism similar to slotted CSMA/CA and use acknowledgments for reliability. In addition to sensing the channel according to the CSMA algorithm, called physical carrier sensing, IEEE 802.11 devices perform virtual carrier sensing by tracking channel utilization with control messages. Each device maintains a counter, called the network allocation vector (NAV), that indicates the channel has activity on it whenever the NAV has a non-zero value. Devices update the NAV based on the data length present in control messages they receive. Periodically, each device decrements its NAV so that the current transmission ends when the NAV reaches zero. Using the NAV allows a device to quickly check for possible channel activity without having to activate the device's transceiver. For the purpose of determining channel activity, an IEEE 802.11 device considers the channel busy whenever physical channel sensing detects a transmission or when the NAV contains a non-zero value.

The DCF in IEEE 802.11 operates similar to slotted CSMA/CA with the use of virtual carrier sensing and acknowledgments. When first trying to transmit a message, a device senses the channel and, if free for a time period, transmits the message. If the device detects activity on the channel it defers access to the current transmission and performs the backoff algorithm. A device using the DCF considers the wireless channel idle if it detects no activity on it for a time period called the DCF interframe space (DIFS). An IEEE 802.11 device performs the backoff algorithm by randomly selecting a number of time slots to wait and storing this value in a backoff counter. For each time slot where the device senses no activity on the channel, it decrements its backoff counter and transmits a frame when the count reaches zero. If the device

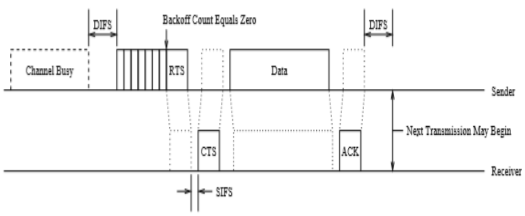

Figure 3. IEEE 802.11

DCF Backoff Algorithm and Message Transferdetects activity on the channel before the backoff counter reaches zero, it halts the countdown, defers access to the current transmission, and continues the countdown after the channel becomes idle for a DIFS. Devices that successfully receive a data message respond by transmitting an acknowledgment after a short interframe space (SIFS). IEEE 802.11 defines a SIFS shorter than a DIFS so that other devices do not physically sense an idle channel and cause a collision by transmitting over a control message. Figure 3, modified from the IEEE 802.11 standard, shows a message transfer when the sender detects channel activity upon the first carrier sense.

The PCF extends the DCF by having the AP coordinate collision-free time periods within its transmission range. The AP prepares for collision-free trans- missions by broadcasting a beacon message that includes a list of devices to receive data during the next time period and an indication of the contention-free period's length. During the contention-free period the AP transmits messages to the devices listed in the beacon or, optionally, transmits polling messages to devices, which allows the devices to initiate data transfer with the AP. Before transmitting messages the AP waits for the channel to become idle for a PCF interframe space (PIFS) and will timeout after this period when it does not receive any expected response from a device. IEEE 802.11 defines the PIFS between the DIFS and SIFS in length; this allows the AP to have priority over devices operating in its range according to the DCF, but allows devices to transmit replies, such as CTS and ACK messages.

IEEE 802.11 does not suit sensor networks due to the differences of the in- tended applications. Characteristics important to devices operating on a wire- less local area network, such as fairness, mobility support, high throughput, and low latency, influenced the design of the IEEE 802.11 standard, but these do not have as high a priority in sensor networks as energy conservation. As a result, IEEE 802.11 devices consume large amounts of energy due to the high percentage of time spent listening without receiving messages [4]. IEEE 802.11 does provide a simple energy management capability, called a power save mode, to devices operating according to the PCF. Devices that wish to sleep inform the AP using special control messages and enter sleep mode when they do not have messages to receive or transmit. Each device wakes up to receive beacon messages from the AP to determine if it must receive messages during the contention-free period and to remain synchronized with the AP. The work [4] provides some discussion of the IEEE 802.11 power save mode and notes the following limitations: power save mode only operates in infrastructure mode, so scalability becomes a problem, and the IEEE 802.11 standard does not specify when or for how long devices should sleep. Additionally, the protocol overhead in IEEE 802.11, which local networks can tolerate, becomes very large when used in sensor networks where applications may only generate a few bytes of data per message.

III. Flooding Protocol

In the case of flooding [5], the source node tries to flood the information to the entire neighborhood in the network. The behavior of all the nodes in the network is exactly same; every node receives the message and after keeping a copy, forwards it to other nodes and this cycle works until the message reaches to sink node.

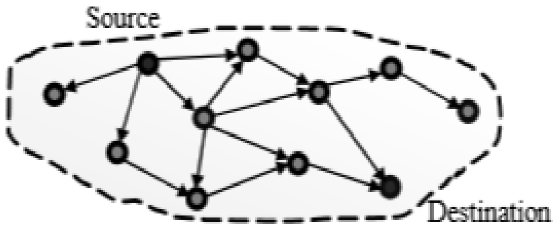

Figure 4. The Flooding Protocol

It is the simplest and most reliable routing technique to route the information to all the nodes in the sensor network. Since the message will be sent to at least once to every host it is almost guaranteed to reach its destination. But the unlimited broadcasting the packets in the flooding scheme will cause the broadcast storm. The flooding routing protocol has three deficiencies as:

• Implosion: Because the nodes in the flooding scheme deliver the packets by broadcasting, the same packet may achieve the same node via different routes. When a sensor node receives a packet, it will not check the packet if it has received the packet before. This character makes the duplicated packets sent to the same place.

• Overlap: When these two sensors detect same event, they may both send a data of this event to the sink. This may cause that the duplicated information of an event is sent to the sink.

• Resource blindness: When a sensor node is not trans- mitting packets in flooding, it doesn't change their actives, even if the sensor nodes don't have much power to operation.

IV Design Model Description.

We have chosen the ns-2 simulator for this research because it realistically models arbitrary node mobility as well as physical radio propagation effects such as signal strength, interference, capture effect, and wireless propagation delay. The simulator also includes an accurate model of the IEEE 802.11 Distributed Coordination Function (DCF) wireless MAC protocol.

- NS2 provides the network simulation environment for both wired, wireless means MANET networks.
- Provides the modules for the wireless channel such as 802.11, 802.16 etc.
- Provides the number of routing protocols for choice in which the routing is done along multiple paths.
- Simulations of the cellular networks possible as the mobile hosts are simulated as well.

The analysis is being done on the basis of the results of *.nam file and the *.tr file. We also evaluate the performance of the protocol. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of message between

the nodes. It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. With the help of 2D and 3D graphs we have tried to analyze the simulation with different simulation time. The scripts for the NAM is stored as *.nam and for trace-graph *.tr is used.

The arriving traffic for a node is modeled using the single source producing packets at rate λ such that,

$$\lambda=\Sigma\lambda i, \ldots \textbf{(1)}$$

where, 'λ' is the arrival rate of the arriving traffic 'i' represents neighboring nodes in the WSN

A. Energy Consumption

The metric is measured as the percent of energy consumed by a node with respect to its initial energy. The initial energy and the final energy left in the node, at the end of the simulation run are measured. The percent energy consumed by a node is calculated as the energy consumed to the initial energy. And finally the percent energy consumed by all the nodes in a scenario is calculated as the average of their individual energy consumption of the nodes.

*Percent_Energy_Consumed = [(InitialEnergy – FinalEnergy) / InitialEnergy] * 100*

Average_Energy_Consumed = Sum_of_Percent_Energy_Consumed_by_All_Nodes / Number_of_Nodes

Residual_Energy = total_energy_given_to_all_nodes – Sum_of_energy_consumed_by_all_nodes.

B.Scenarios

There number scenario and traffic files needs to generate in order to evaluate the performance of the routing protocols under the different network conditions. In this simulation the main parameter which is varied during the simulation is the number of nodes, number of connections and size of the network.

Following are parameters which are varied for these simulations:

_ Nodes of maximum velocity

_ Maximum number of data connections

_ Number of nodes

_Size network area

1) 10 nodes

2) 20 nodes

3) 30 nodes

4) 40 nodes

Number of Nodes	10
Traffic Patterns	CBR (Constant Bit Rate)
Network Size	500 x 500 (X x Y)
Max Speed	10 m/s
Simulation Time	15s
Transmission Packet Rate Time	10 m/s
Pause Time	2.0s
Routing Protocol	FLOODING
MAC Protocol	802.11

Number of Nodes	20
Traffic Patterns	CBR (Constant Bit Rate)
Network Size	1000 x 1000 (X x Y)
Max Speed	10 m/s
Simulation Time	20s
Transmission Packet Rate Time	10 m/s
Pause Time	2.0s
Routing Protocol	FLOODING
MAC Protocol	802.11

Number of Nodes	30
Traffic Patterns	CBR (Constant Bit Rate)
Network Size	1000 x 1000 (X x Y)
Max Speed	10 m/s
Simulation Time	25s
Transmission Packet Rate Time	10 m/s
Pause Time	2.0s
Routing Protocol	FLOODING
MAC Protocol	802.11

Number of Nodes	40
Traffic Patterns	CBR (Constant Bit Rate)
Network Size	1000 x 1000 (X x Y)
Max Speed	10 m/s
Simulation Time	25s
Transmission Packet Rate Time	10 m/s
Pause Time	2.0s
Routing Protocol	FLOODING
MAC Protocol	802.11

C. Software Requirements

For the simulation of this work we have to need the following setups requirement for the same

1) Cygwin: for the windows XP
2) Ns-allinone-2.31: AODV/DSDV protocol is simulated using this versions

Following are the steps to for installation of the Cygwin + ns2

1) Computer Requirements
   a. 5 GB free space of HDD
   b. 1 GB of RAM
2) Installation Assumptions
   a. Windows is installed in C drive.
3) Installing Cygwin as following ways:
   a. download the latest version Cygwin setup.
   b. execute the Cygwin setup

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 8, August - 2013

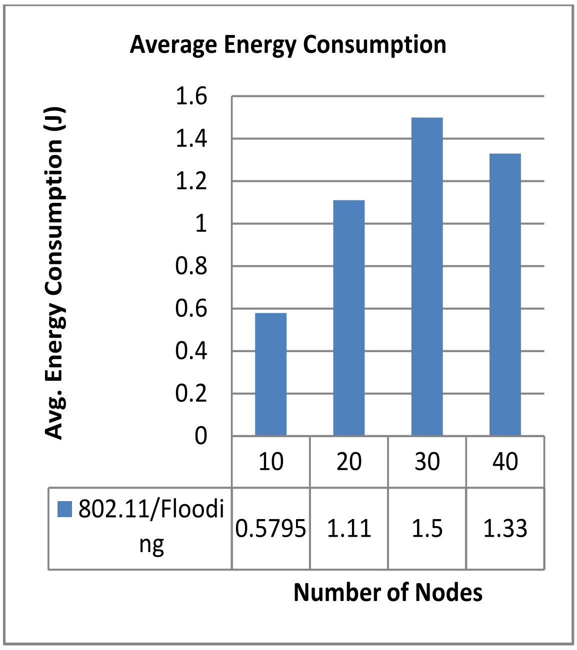

Figure 5. Average Energy Consumption Performance Analysis

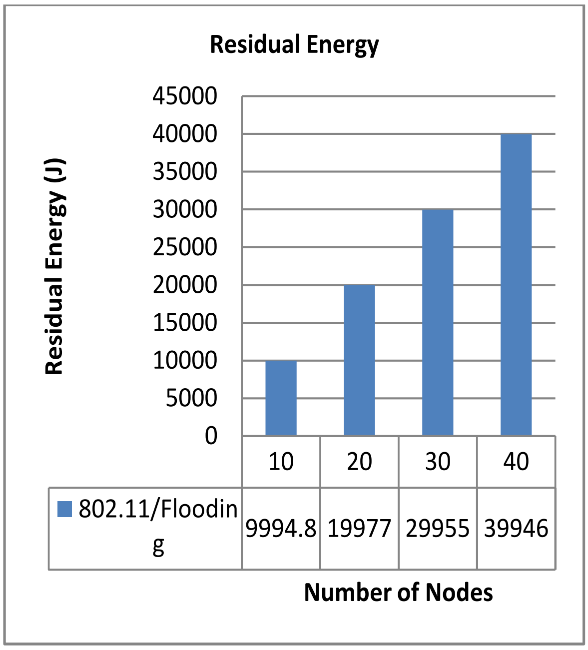

Figure 6. Residual Energy Performance Analysis

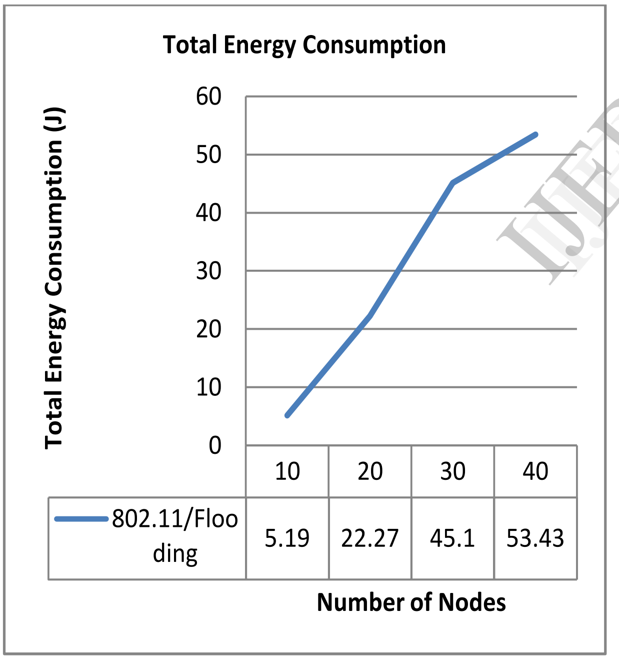

Figure 7. Total Energy Consumption Performance Analysis

VI. Conclusions and Future work

We conclude this paper by summarizing the research discussed in the previous sections, followed by a section on directions for future research. We have proposed a cross-layer design that exploits the characteristics of sensor networks where the standard MAC protocol has been cross layered with flooding as a routing protocol and evaluated the energy consumption by simulation. Our paper presents a method for increased scalability and network wide energy-efficiency in WSNs. Each time the nodes in the network configure – new/hibernating nodes get discovered by the local search performed as a part of the dynamic clustering scheme – an interesting feature of our paper – giving a relatively superior scalability capability to WSNs in comparison to existing procedures. , we observe that energy consumption using our scheme for low traffic is very low – this is very good as WSNs generally operate under event-driven detections, and traffic during the entire lifetime of the network is generally very low.

Finally, it will be important to develop secure communication for WSNs. End-users need to be able to ensure unauthorized users cannot access the data from the sensor networks. We can modify theStandard MAC protocol and flooding protocol so to conserve more energy. Furthermore, the importance of mobility in sensor networks and schemes focused on the energy implications of node mobility will also need to be addressed.

References

[1] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, pages 259_268, New York, NY, USA, 2004. ACM.

[2] Holger Karl and Andreas Willig. "Protocols and architectures for Wireless Sensor Networks", Wiley, 2005, ISBN:0470095105.

[3] IEEE, IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999).

[4] W. Ye, J. Heidemann, D. Estrin, Medium access control with coordinated adaptive sleeping for wireless sensor networks, IEEE/ACM Transactions on Networking 12 (3) (2004) 493–506.

[5] Wei Yen, Ching Chen and Cheng Yang, "Single Gossiping with Directional Flooding Routing Protocol in WSNs", IEEE, 2008.