الجامعة اللبنانية
UNIVERSITE LIBANAISE

Wireless Sensor Network

Mobility aware simulation project for WSN using OMNET ++ network simulator

Presented for:

Dr.A.Samhat

Presented by:

Mohammad Haidar 3967

Summary:

List of figures and tables:

1.Introduction:

1.1.What is the wireless sensor network?

A wireless sensor network (WSN) is composed of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

1.2.Usage and application of WSN

It seems like it was not so long ago that there was a serious debate over whether or not wireless sensor networks — and wireless communications in general — were a suitable technology. If you take a look around, that debate is over.

The increased adoption of wireless sensors is due, like most technologies, to solid, practical reasons. Chief among these reasons is ease of implementation (no long cable runs), ability to operate in harsh environments, easy troubleshooting and repair, and high levels of performance.

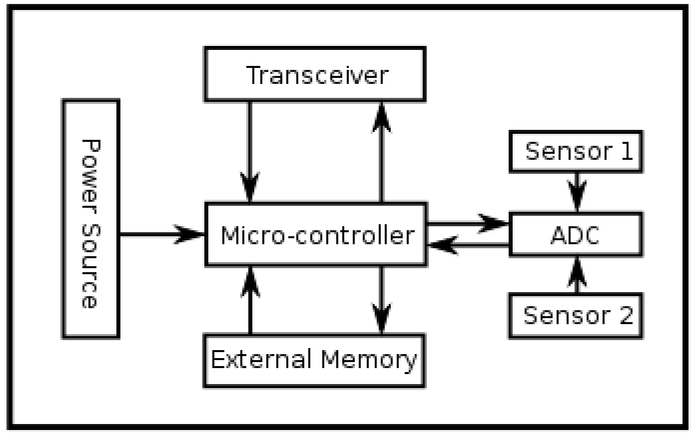
Most common application :

1. Military Applications: Counter sniper System for Urban Warfare. It detects and accurately locates shooters even in urban environments.
2. Industrial Applications: Robotics, Monitoring and Energy Usage Evaluation for Electric Machines, Industrial control … and many more.
3. Environmental Applications: Habitat Monitoring, Volcano Monitoring, Underground Structure Monitoring (mines), Precision Agriculture.
4. Healthcare Applications: Remote monitoring capability, Real-time identification and action taking, being able to identify the context.
5. Daily life Applications: Intelligent Car Park Management, Smart home, Smart work.

2.WSN Node Model:

Functionally, smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, power supply, a radio interface, and some additional components depending on the need.

2.1. Controller



The controller performs tasks, processes data and controls the functionality of other components in the sensor node. While the most common controller is a microcontroller, other alternatives that can be used as a controller are: a general purpose desktop microprocessor, digital signal processors, FPGAs and ASICs. A microcontroller is often used in many embedded systems such as sensor nodes because of its low cost, flexibility to connect to other devices, ease of programming, and low power consumption. A general purpose microprocessor generally has a higher power consumption than a microcontroller, therefore it is often not considered a suitable choice for a sensor node. Digital Signal Processors may be chosen for broadband wireless communication applications, but in Wireless Sensor Networks the wireless communication is often modest: i.e., simpler, easier to process modulation and the signal processing tasks of actual sensing of data is less complicated. Therefore the advantages of DSPs are not usually of much importance to wireless sensor nodes. FPGAs can be reprogrammed and reconfigured according to requirements, but this takes more time and energy than desired.

2.2. Transceiver

Sensor nodes often make use of ISM band, which gives free radio, spectrum allocation and global availability. The possible choices of wireless transmission media are radio frequency (RF), optical communication (laser) and infrared. Lasers require less energy, but need line-of-sight for communication and are sensitive to atmospheric conditions. Infrared, like lasers, needs no antenna but it is limited in its broadcasting capacity. Radio frequency-based communication is the most relevant that fits most of the WSN applications. WSNs tend to use license-free communication frequencies: 173, 433, 868, and 915 MHz; and 2.4 GHz. The functionality of both transmitter and receiver are combined into a single device known as a transceiver. Transceivers often lack unique identifiers. The operational states are transmit, receive, idle, and sleep. Current generation transceivers have built-in state machines that perform some operations automatically.

Most transceivers operating in idle mode have a power consumption almost equal to the power consumed in receive mode. Thus, it is better to completely shut down the transceiver rather than leave it in the idle mode when it is not transmitting or receiving. A significant amount of power is consumed when switching from sleep mode to transmit mode in order to transmit a packet.

2.3. External memory

From an energy perspective, the most relevant kinds of memory are the on-chip memory of a microcontroller and Flash memory—off-chip RAM is rarely, if ever, used. Flash memories are used due to their cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage are: user memory used for storing application related or personal data, and program memory used for programming the device. Program memory also contains identification data of the device if present.

2.4. Power source

A wireless sensor node is a popular solution when it is difficult or impossible to run a mains supply to the sensor node. However, since the wireless sensor node is often placed in a hard-to-reach location, changing the battery regularly can be costly and inconvenient. An important aspect in the development of a wireless sensor node is ensuring that there is always adequate energy available to power the system. The sensor node consumes power for sensing, communicating and data processing. More energy is required for data communication than any other process. The energy cost of transmitting 1 Kb a distance of 100 metres (330 ft) is approximately the same as that used for the execution of 3 million instructions by a 100 million instructions per second/W processor. Power is stored either in batteries or capacitors. Batteries, both rechargeable and non-rechargeable, are the main source of power supply for sensor nodes. They are also classified according to electrochemical material used for the electrodes such as NiCd (nickel-cadmium), NiZn (nickel-zinc), NiMH (nickel-metal hydride), and lithium-ion. Current sensors are able to renew their energy from solar sources, temperature differences, or vibration. Two power saving policies used are Dynamic Power Management (DPM) and Dynamic Voltage Scaling (DVS). DPM conserves power by shutting down parts of the sensor node which are not currently used or active. A DVS scheme varies the power levels within the sensor node depending on the non-deterministic workload. By varying the voltage along with the frequency, it is possible to obtain quadratic reduction in power consumption.

2.5. Sensors

Sensors are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. A sensor node should be small in size, consume extremely low energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

Sensors are classified into three categories: passive, omni-directional sensors; passive, narrow-beam sensors; and active sensors. Passive sensors sense the data without actually manipulating the environment by active probing. They are self powered; that is, energy is needed only to amplify their analog signal. Active sensors actively probe the environment, for example, a sonar or radar sensor, and they require continuous energy from a power source. Narrow-beam sensors have a well-defined notion of direction of measurement, similar to a camera. Omni-directional sensors have no notion of direction involved in their measurements.

The overall theoretical work on WSNs works with passive, omni-directional sensors. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing. Several sources of power consumption in sensors are: signal sampling and conversion of physical signals to electrical ones, signal conditioning, and analog-to-digital conversion.

Spatial density of sensor nodes in the field may be as high as 20 nodes per cubic meter.

2.6. Specifications of Sensor Nodes

All of these subunits may need to fit into a matchbox-sized module whose size may be smaller than even a cubic centimeter. Added to size, there are also some other stringent specifications of sensor nodes:

- Consume extremely low power.
- Operate in high volumetric densities.
- Have low production cost, can be easily replaced, and the malfunction of any does not halt other sensors.
- Are autonomous and operate unattended.
- Are adaptive to the environment.

Fig.2b

2.7. Performance Metrics of WSNs

- <u>Network lifetime:</u> It is measure of energy efficiency, as sensor nodes are battery operated.

- <u>Energy consumption:</u> It is the sum of used energy by all WSN nodes.

- <u>Latency:</u> It is the end-to-end delay that implies the average time between sending a packet from the source, and the time for successfully receiving the message at the destination.

- Accuracy: It is the freedom from mistake or error, correctness, conformity to truth, exactness.

- Fault-tolerance: The WSN must be fault-tolerant such that non-serious failures are hidden from the application in a way that does not hinder it.

- Scalability: It is WSN adaptability to increased workload, that is to include more sensor nodes than what was anticipated during network design.

- Network throughput: It is a common metric. The end-to-end throughput measures the number of packets per second received at the destination.

- Success rate: It is also a common metric. It is the total number of packets received at the destinations verses the total number of packets sent from the source.

3.WSNs protocols

3.1. Layers Functions

- The physical layer: is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption.

- The data link layer: is responsible for the multiplexing of data streams, data frame detection, medium access and error control. It ensures reliable point-to-point and point-to-multipoint

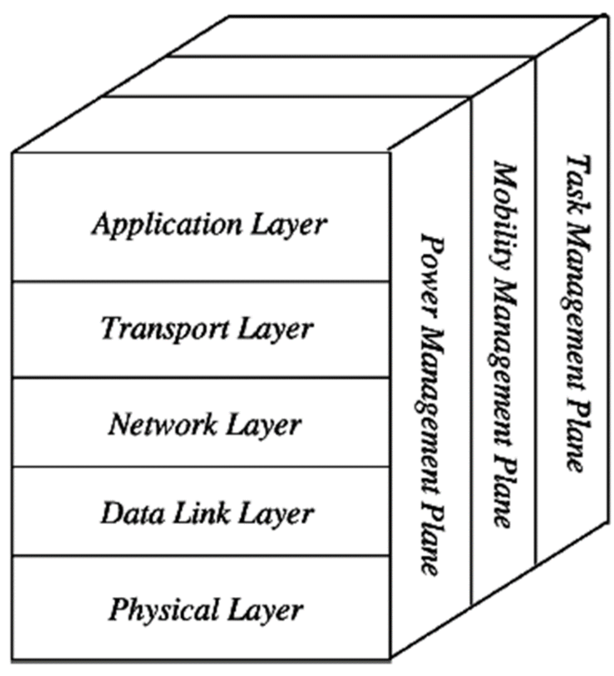


Fig.3a

connections in a communication network.

- <u>The network layer:</u> takes care of routing the data supplied by the transport layer. The network layer design in WSNs must consider the power efficiency, data-centric communication, data aggregation, etc.

- <u>The transportation layer:</u> helps to maintain the data flow and may be important if WSNs are planned to be accessed through the Internet or other external networks.

- <u>The application layer:</u> depending on the sensing tasks, different types of application software can be set up and used on the application layer.

3.2. Standards

Wireless sensor standards have been developed with a key design requirement for low power consumption. The standards define the functions and protocols necessary for sensor nodes to interface with a variety of networks.

3.3. IEEE 802 Standards

	802.11b WLAN	**802.15.1 WPAN**	**802.15.4 LR-WPAN**
Range	~100 m	~10 - 100 m	10 m
Raw data rate	11 Mbps	1 Mbps	<= 0.25 Mbps
Power Consumption	medium	low	Ultra low

Table 3a

The IEEE 802.15 is a working group focusing on wireless personal area networks (WPANs), it has seven different approved standards and several

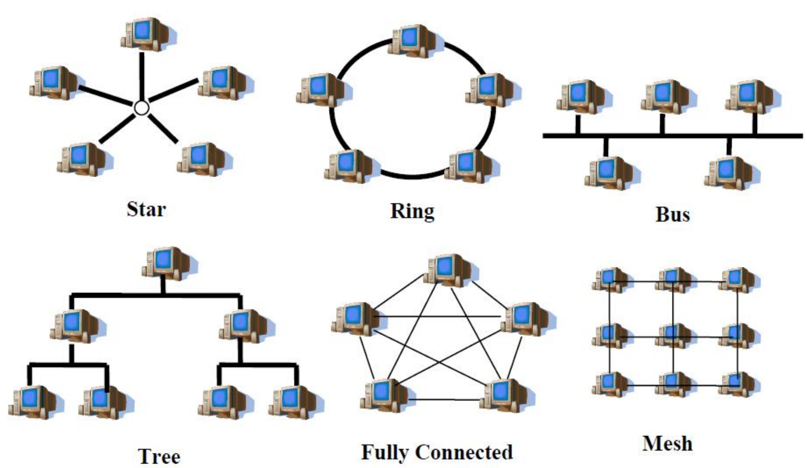
ongoing standards discussions which are in different phases of the standardization process.
All 802.15.x approved standards propose PHY and MAC layers, they do not provide network, transport or application layers, implying that this task is left for other parties.

4.WSNs Topologies

4.1.Network topology

The basic issue in communication networks is the transmission of messages to achieve a prescribed message throughput (Quantity of Service) and Quality of Service (QoS). QoS can be specified in terms of message delay, message due dates, bit error rates, packet loss, economic cost of transmission, transmission power, etc. Depending on QoS, the installation environment, economic considerations, and the application, one of several basic network topologies may be used.

A communication network is composed of nodes, each of which has computing power and can transmit and receive messages over communication links, wireless or cabled. The basic network topologies are shown in the figure and include fully connected, mesh, star, ring, tree, bus. A single network may consist of several interconnected subnets of different topologies.



Networks are further classified as Local Area Networks (LAN), e.g. inside one building, or Wide Area Networks (WAN), e.g. between buildings.

- Fully connected networks: suffer from problems of NP-complexity [Garey 1979]; as additional nodes are added, the number of links increases exponentially. Therefore, for large networks, the routing problem is computationally intractable even with the availability of large amounts of computing power.

- Mesh networks: are regularly distributed networks that generally allow transmission only to a node's nearest neighbors. The nodes in these networks are generally identical, so that mesh nets are also referred to as peer-to-peer (see below) nets. Mesh nets can be good models for large-scale networks of wireless sensors that are distributed over a geographic region, e.g. personnel or vehicle security surveillance systems. Note that the regular structure reflects the communications topology; the actual geographic distribution of the nodes need not be a regular mesh. Since there are generally multiple routing paths between nodes, these nets are robust to failure of individual nodes or links. An advantage of mesh nets is that, although all nodes may be identical and have the same computing and transmission capabilities, certain nodes can be designated as 'group leaders' that take on additional functions. If a group leader is disabled, another node can then take over these duties.

- Star topology: All nodes of the star topology are connected to a single hub node. The hub requires greater message handling, routing, and decision-making capabilities than the other nodes. If a communication link is cut, it only affects one node. However, if the hub is incapacitated the network is destroyed.

- Ring topology: In the ring topology all nodes perform the same function and there is no leader node. Messages generally travel around the ring in a single direction. However, if the ring is cut, all communication is lost.

5.Energy consumption

Energy has always been a critical issue in wireless sensor networks (WSNs) because sensor nodes are usually deployed in an environment where replacement of batteries is not only costly but also laborious. WSNs are mainly handicapped by the energy consumption due to both transmission and reception powers of the underlying sensor nodes. The simplicity of 802.11 not withstanding its fixed transmission power consumption leads to wastage of considerable network throughput.

With ad hoc WSNs, control of transmission power consumption is thus quintessential for two obvious reasons, namely the avoidance of battery power wastage and enhanced throughput .

While dealing with WSNs, a fair number of researchers have kept energy consumption as their primary goal while treating the network throughput as a secondary issue. Other things apart, using variable transmission powers can lead to both increased network lifetime and throughput. As far as network topology is concerned, clustering-based sensor networks have shown better results in terms of network throughput and energy consumption but they are limited by the fact that the nodes consume constant transmission power independent of their distance from the cluster-head which not only results in energy wastage but also decreases network throughput.

6.Mobility

Wireless sensor network (WSN) is an emerging class of ad hoc networks. WSNs comprise sensor nodes distributed over geographic area to monitor certain phenomenon. The sink node (base station) acts as gateway and is comparatively resourceful, whereas, sensor nodes have constrained energy, processing capacity, and memory.

Previous studies mostly consider evaluation based on static networks. There are various applications where nodes are mobile and needs due consideration. Mobile sensor network applications include battlefield surveillance, habitat monitoring, and search and rescue operations. Routing in mobile WSNs becomes more difficult because of the frequent path failures and unpredictable topology changes, which may increase packet loss and packet delay. Different routing protocols exist that can be broadly classified into hierarchical and flat routing. Some of the flat routing protocols are not scalable due to the assumption that sensor nodes can directly send data to the sink node. Therefore, hierarchical routing protocols are preferred if scalability is the deciding factor or the number of nodes is very high.

When nodes are mobile, the performance of hierarchical (clustering based) protocols suffers due to two main reasons i.e., path breakage and consequently packet loss during intra cluster and inter cluster communication.

Protocols having no backup strategy to deal with such situation yield low packet delivery ratio. Mostly the existing comparative studies consider only one mobility model for evaluating routing protocols. Only one mobility model does not reflect the true behavior of a protocol, therefore we have tested the selected protocols with three different mobility models.

6.1.Routing protocols

One of the most important design goals of WSNs is to minimizing energy consumption of the network. Moreover, if sensor nodes are mobile, it further complicates the design of the network. To comprehensively simulate a newly proposed protocol for mobile sensor networks, it is recommended to check the performance of the protocol with multiple mobility models. This is because performance of every protocol is dependent on the application scenario. A given protocol can perform well in one environment and can fail when environment is changed. Same is the case with mobility models. A given protocol can perform well for one mobility model but can exhibit deteriorated performance under some other mobility model. This is because the performance of mobile WSN routing protocols is highly affected by the mobility models.

1. **Position Based Protocols:**

   Position based routing protocols are dependent on the location information. Location of sensor nodes can be identified with the help of low power GPS module embedded in sensor nodes or some distributed localization technique .By using location information, many tasks can be done efficiently. For example, based on the distance between two nodes, energy consumption can be estimated for all routing paths between the two nodes and then select more energy efficient path. Position based routing protocols, that are considered during our work are Mobility Aware Routing Protocol (MAR) and Distributed Geographic Clustering Protocol (GRC).

- <u>Mobility Aware Routing Protocol (MAR):</u>
  In MAR, cluster heads are selected on the basis of mobility. Nodes which are less mobile are selected as cluster heads and this mechanism of cluster head selection leads to more stable clusters. MAR does not consider residual energy of nodes during selection of cluster heads hence are energy unaware. Moreover, due to mobility of sensor nodes, cluster heads may move out of transmission range of each other. Also MAR does not have any packet recovery mechanism for inter-cluster communication and is location unaware, so packet loss occurs.

- <u>Distributed Geographic Robust Clustering Protocol (GRC):</u>
  GRC is energy aware routing protocol and uses location information for selection of cluster head. Those nodes which are more close to center of specified zones and have higher residual energy are selected as cluster heads. The purpose of introducing “center-ness” factor in selection of cluster heads was to make sure that even if there is mobility, the head will take some time to have substantial movement and get out of the range of the cluster nodes.
  To minimize packet loss during inter-cluster communication a recovery mechanism was introduced in GRC. Two versions of GRC are used during simulations which are GRC without recovery strategy and GRC with recovery strategy (GRC-R).

2. **Non Position Based Protocols**
   Non position based routing protocols do not need any position information to make their routing decisions. Non position based routing protocols, that we have selected includes Distributed

Efficient Clustering Approach (DECA) and Distributed Efficient Multi hop Clustering protocol (DEMC).

- Distributed Efficient Clustering Approach (DECA):
  DECA is a non position-based protocol that considers node mobility, node residual energy, identifier, and its connectivity with other nodes; all these parameters are used to calculate weight for each node. Only one message is transmitted during clustering, which saves more energy as compared to low energy adaptive cluster hierarchy (LEACH) and Hybrid Energy Efficient Distributed Clustering (HEED) which sends multiple clustering messages during clustering phase As transmission and reception are main sources of energy consumption in sensor networks, so by reducing number of messages; DECA becomes more energy efficient. But the major problem with DECA is that it does not use any recover mechanism for inter-cluster communication resulting in packet loss.

- Distributed Efficient Multi hop Clustering protocol (DEMC):
  DEMC is a distributed clustering based routing protocol specially designed for mobile sensor networks and is more energy efficient compared to DECA. This is because DEMC does not send periodic hello messages, does not keep neighbors list and requires only one message per cluster for selection of cluster head. By removing extra overhead and minimizing control messages, DEMC is more energy efficient in comparison to DECA. To minimize inter-cluster communication packet loss, a recovery mechanism was also introduced in DEMC. Therefore, DEMC also incurs less packet loss compared to DECA. Two versions of DEMC were used during simulation. One is simple DEMC without recovery strategy and the other is DEMC with recovery strategy.

6.2. Comparison Strategy

1. **Performance Metrics**
   - Percentage of Packet loss: With this performance metric we can check reliability of a protocol, the lower the percentage of packet loss the more reliable it is. Let ‘n’ be the total packets sent and ‘m’ be the received packets then percentage packet loss is calculated as

     $$((n - m) / n) \times 100 \qquad (1)$$

     We can calculate percentage of packet loss by dividing total number of lost packets by total number of sent packets. When comparing multiple protocols, the one which has lower percentage for packet loss is considered better compared to those which have high percentage of packet loss.

   - Packet delivery ratio: This is also one of the good performance metrics and is calculated by dividing total number of delivered packets by total number of sent packets. For any good protocol the ideal packet deliver ratio must be one. For some protocols packet delivery ratio can be higher than one which is also not a good sign because in that case packet duplication is occurring. So, one must try to achieve packet delivery ratio closer to one but not greater than one. The closer the packet delivery ratio to one, the better the protocol performance is.
2. **Mobility Models**
   The following three mobility models were used during simulations.
   - Linear Mobility Model: In linear mobility model nodes move in a straight line with a certain angle and this angle changes only when the mobile node hits a wall: then it reflects off the wall at the same angle.

- <u>Mass Mobility Model:</u> Mass mobility model is a variant of random waypoint mobility model. In this mobility model nodes are considered to be having some mass and then apply momentum accordingly. Due to this factor, nodes do not turn, starts, or stops instantaneously.

- <u>Random Way Point Mobility Model:</u> In random way point mobility model, nodes move with random speed towards randomly selected destination. As random waypoint mobility model does not consider mass of node so in this mobility model nodes can turn, start, and stop instantaneously.

7.Simulations and results

7.1.Nodes model

The node model is like described above , contains application layer, presentation layer, session layer, transport layer, network layer (the network card nic includes mac layer and physical), and a battery unit plus a mobility unit.

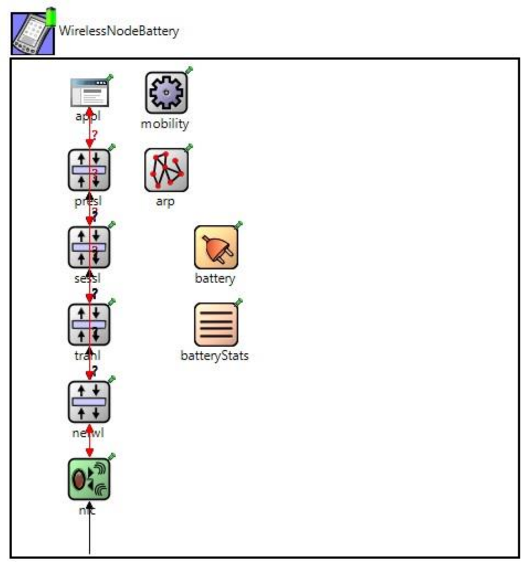


Fig. 7a

7.2.Network topology

We uses in the simulation mesh topology for the simulation of static nodes.

And fully connected network for the mobility simulation.

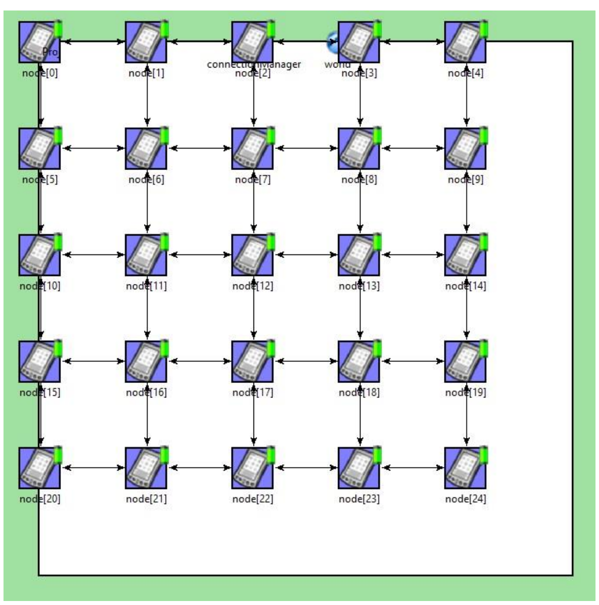


Fig. 7b mesh network

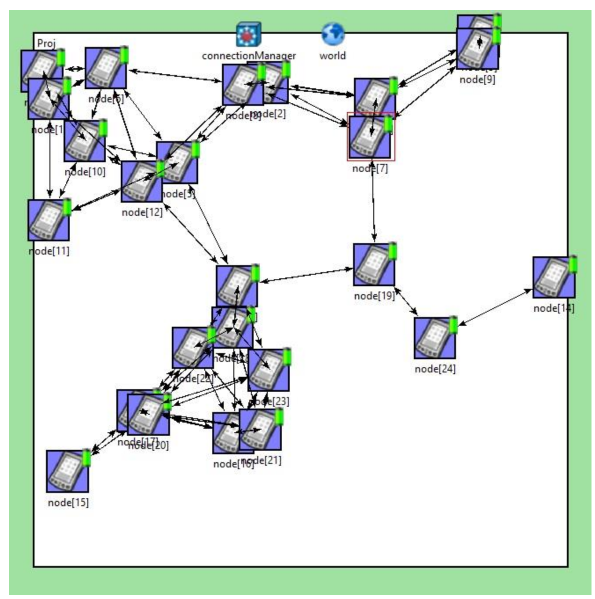


Fig. 7c fully connected network

7.3.Simulation parameters

- Number of nodes : 25
- Ground size : 520mx520m
- Application layer type : Sensor application
- Traffic Type : Periodic
- Number of packets sent by each node : 50
- MAC protocol : CSMA
- Mobility type : Linear Mobility / Mass Mobility / Random Way Point Mobility.
- Mobility speed : varies from 1 to 25 mps.

7.4.Results

Percentage packet loss with random waypoint mobility model:

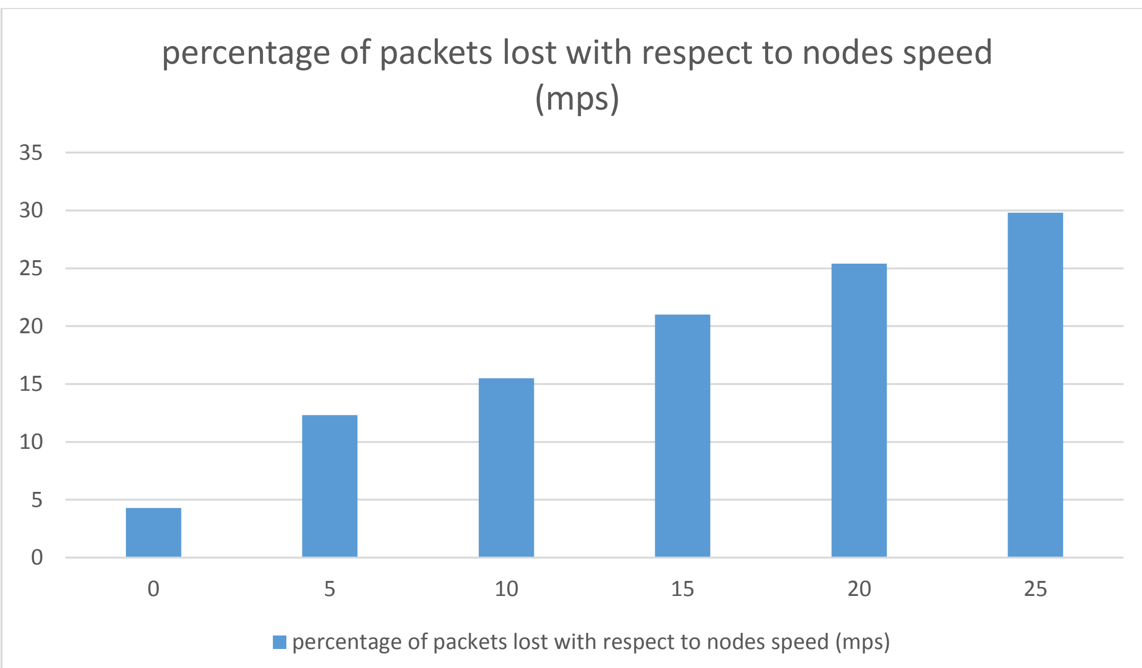


Table 7a Percentage packet loss with random waypoint mobility model:

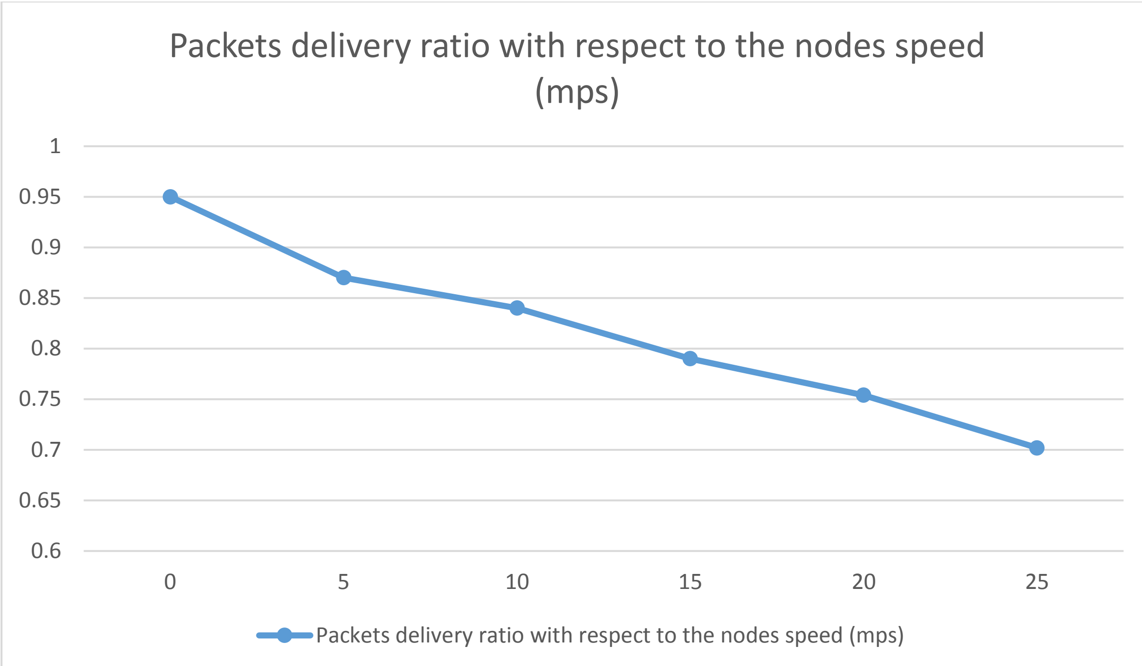


Table 7b Packet delivery ratio with random waypoint mobility model

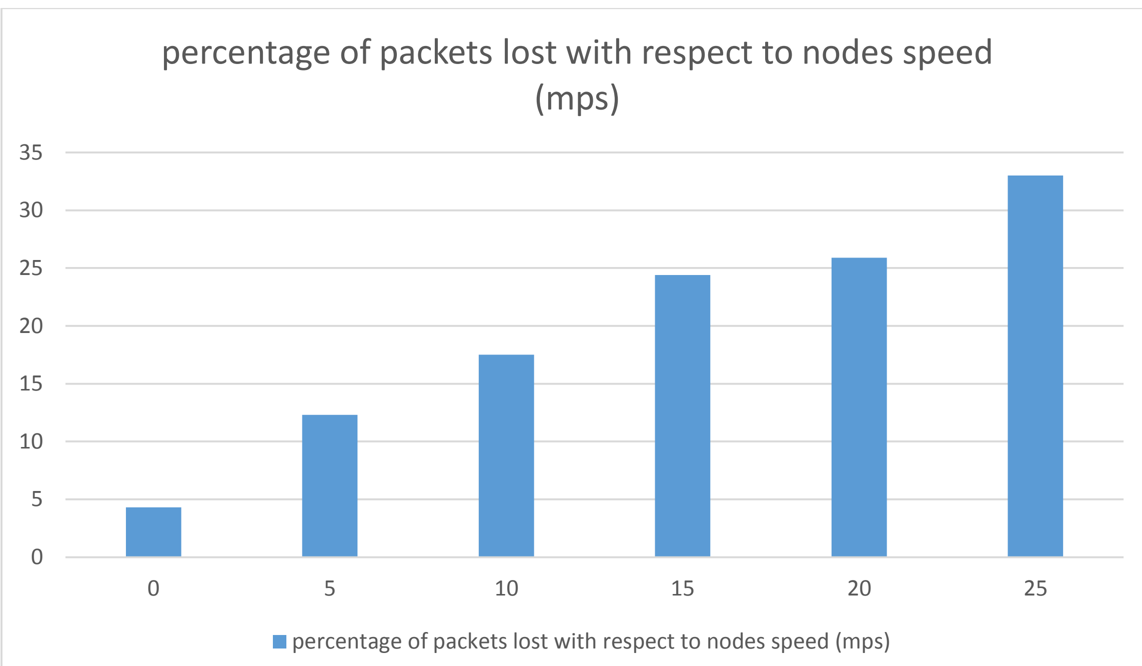


Table 7c Percentage packet loss with respect to mass mobility model

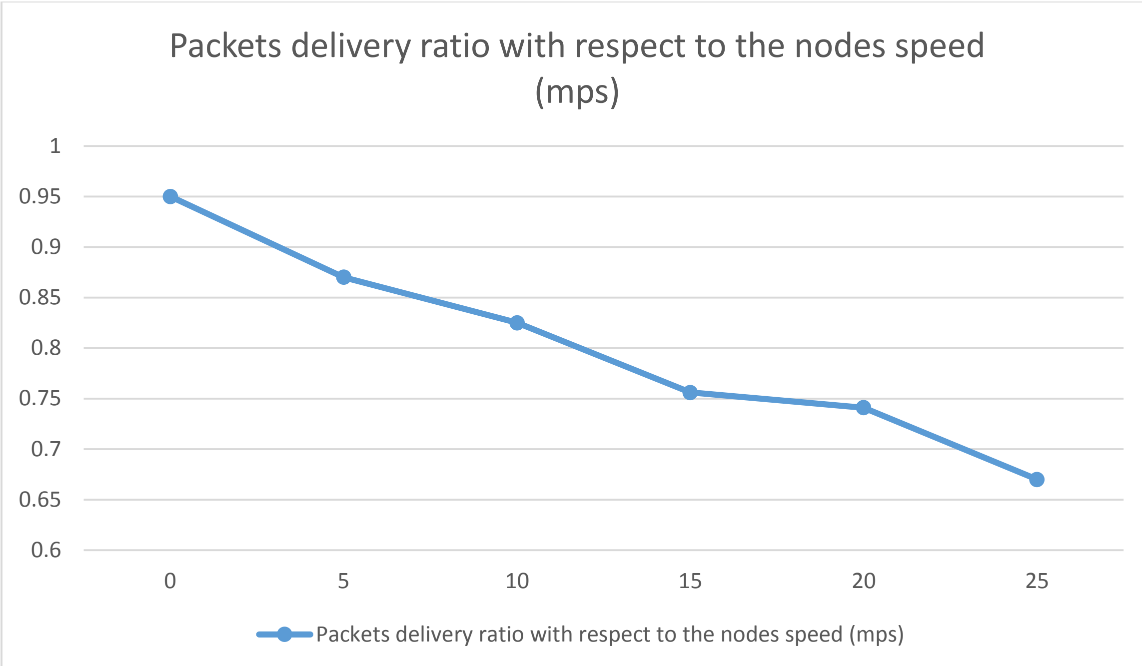


Table 7d Packet delivery ratio with respect to mass mobility model

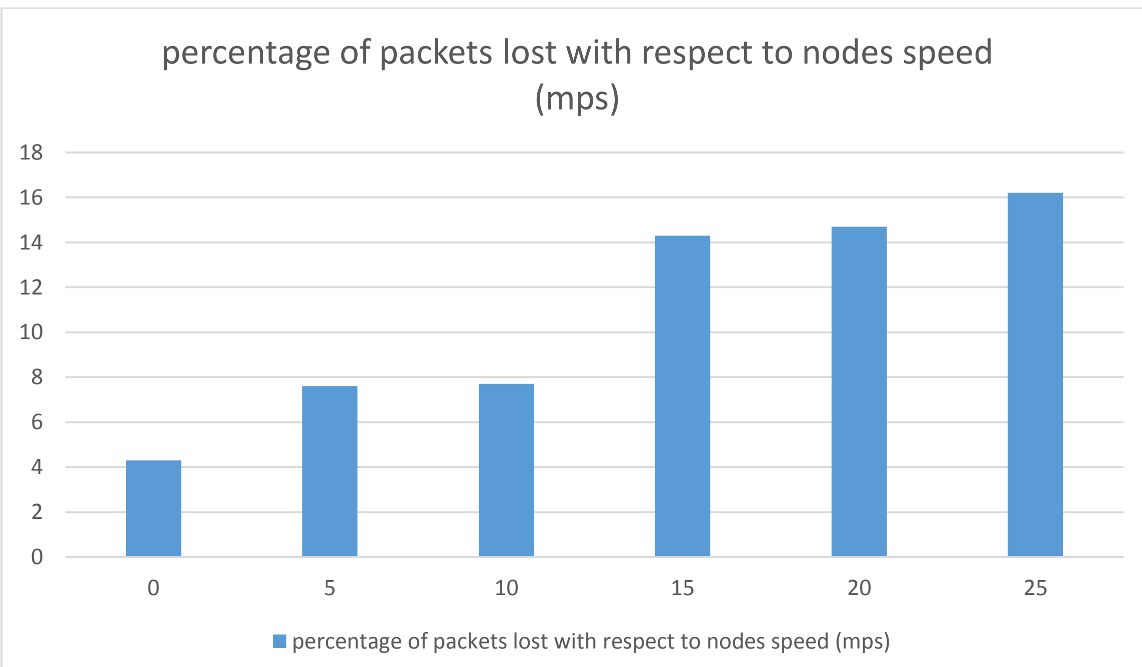


Table 7e Percentage packet loss with respect to linear mobility model

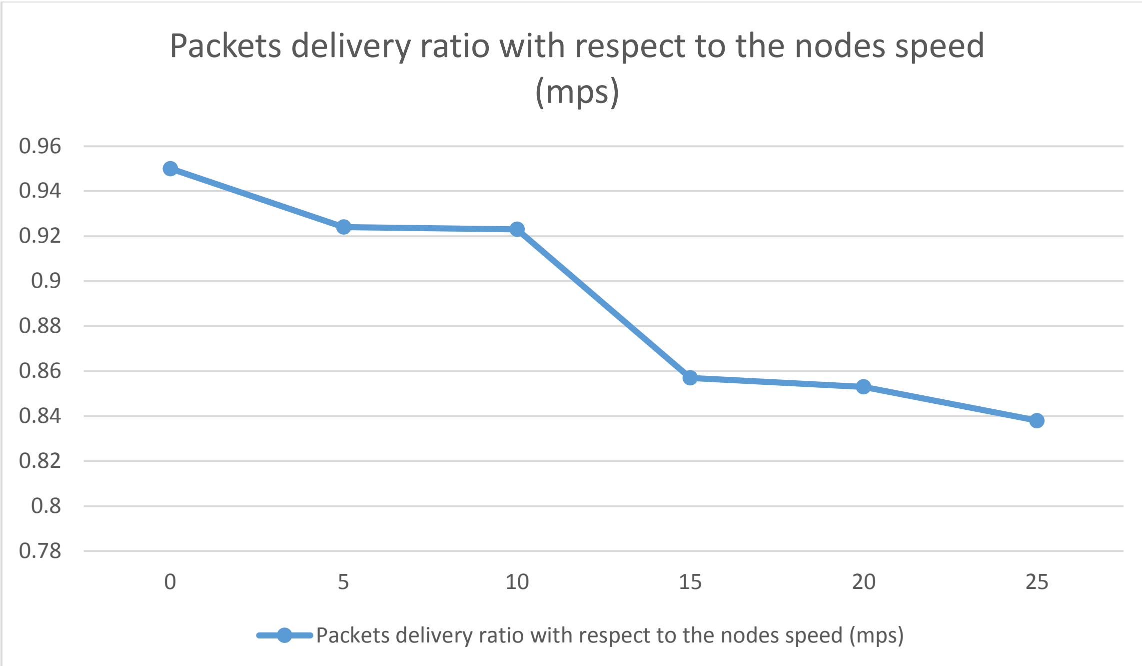


Table 7f Packet delivery ratio with respect to linear mobility model

In random waypoint mobility model, nodes stops a random locations and perform abrupt turns, during these turns, mostly the direction is toward cluster-head. For this reason packet loss of random waypoint mobility model I less compared to mass mobility model. With linear mobility model all protocols have shown minimal packet loss. This is because mobility of all nodes is not only associated with each other but also they move in a straight line until they hit some fixed object. After hitting any fixe point all nodes turn with specific angle and goes in some other direction. In this way nodes mostly move together not away from each which leads to less packet loss a high packet delivery ratio.

8.Conclusion

In this simulation we compared different mobility types and different mobility speeds and recorded the packet loss and delivery ratio to conclude that the packet loss is very low in static WSN but with mobile networks, it increases with the speed of mobility and especially with mass mobility, thus new and efficient routing protocols are necessary for solving this problem and to minimize energy consumption.

References:

- http://www.automationworld.com/

- Y. Xu, J. Heidemann, and D. Estrin, Geography-informed energy conservation for ad hoc routing, in Proc. Mobicom, 2001, pp. 70–84

- Dynamic Power Management in Wireless Sensor Networks, Amit Sinha and Anantha Chandrakasan, IEEE Design & Test of Computers, Vol. 18, No. 2, March–April 2001

- Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010

- http://en.wikipedia.org/

- Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007