Performance Metrics in Ad-hoc Network

Joni Birla[1], Basant Sah[2]
[1] M. Tech Student , , BRCM, Bahal
[2]Assistant Professor , BRCM, Bahal
jonibirla@yahoo.com
basantbitmtech2008@gmail.com

Abstract— **In last few years there has been significant growth in the area of wireless communication. Quality of Service (QoS) has become an important consideration for supporting variety of applications that utilize the network resources. These applications include voice over IP, multimedia services like video streaming, video conferencing etc.. This paper aims on performance Metrics as implemented by Ad-hoc networks. In real life we use voice call, video streaming which are set up through Wireless Sensor Network. We use many parameters for quality of service and these are: throughput, packet loss, average jitter and average delay. WSN is the part of Adhoc Network in which we don't have intelligent nodes. Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks.**

Index Terms—**Improvement over WSN, Quality of services in Ad-hoc Network, Performance Metrics used in WSN, Characteristics of WSN**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks. There is no concept of fixed base station. So, each node in the network acts as a router to forward the packets to the next node. Wireless networks are capable of handling of topology changes and malfunctions in nodes. It is fixed through network reconfiguration. For instance, if the node leaves the network and causes link breakages, affected nodes can request new routes and problem will be solved. This will slightly increase the delay, but the network will still be operational. It is the technology aimed to provide broadband wireless data access over long distances. This technology provides basic Internet Protocol (IP) connectivity to the user. The variety of applications used in IP networks has increased tremendously in the recent years. Various multimedia applications along with the common email, file transfer and web browsing applications are becoming increasingly popular. These applications send large audio and video streams with variable bandwidth and delay requirements. On the other hand, remote monitoring of critical services such as E-commerce and banking applications which do not need strict bandwidth guarantees due to the good nature of the data transfer. Instead, these applications require reliable and prompt packet routing. The presence of different kinds of applications in a network, results in heterogeneous traffic load. The traffic from different applications may require certain type of quality of service. In this paper, the Performance Metrics as prescribed in the Wireless Sensor networks is studied.

As packets travel within a wireless network such as WSN, they experience the following problems: Delay, jitter, out-of-order delivery, packet loss or error.

Quality of Service refers to the probability of the telecommunication network meeting a given traffic contract. In the field of packet-switched networks and computer networking it is used informally to refer to the probability of a packet succeeding in passing between two points in the network. Although the name suggests that it is a qualitative measure of how reliable and consistent a network is, there are a number of parameters that can be used to measure it quantitatively. These include throughput, transmission delay or packet delay, delay jitter, percentage of packets lost etc.

Quality of service enables end-to-end IP based QoS. Among other things, the MAC layer is responsible for scheduling of bandwidth for different users. The MAC layer performs bandwidth allocation based on user requirements as well as their QoS profiles. The standard is designed to support a wide range of applications. These applications may require different levels of QoS. To accommodate these applications, the WSN has defined many service flow classes.

These service flows can be created, changed, or deleted by the issuing Dynamic Service Addition (DSA), Dynamic Service Change (DSC), and Dynamic Service Deletion (DSD) messages. Each of these actions can be initiated by the Subscriber Station (SS) or the Base Station (BS) and are carried out through a two or three-way-handshake.

Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks. These applications send large audio and video streams with variable bandwidth. The services classes defined by Wireless Sensor

Network are given below:
This paper focuses on the performance Metrics in Wireless sensor networks.. To analyze the QoS parameters simulation based on the popular network simulator ns-2 is used. Various parameters that determine QoS of real life usage scenarios and traffic flows of applications is analyzed. The goal is to compare different types of service flows with respect to the QoS parameters such as throughput, average jitter, average delay and packet loss, end to end delay, energy, Packet delivery fraction.

SERVICE CLASSES DEFINED BY WSN

	Description	**Applications**
Unsolicited Grant Service	For Constant Bit Rate (CBR) and delay-dependent applications	VOIP
Real-Time Polling Service	For Variable Rate and delay dependent applications	Streaming audio, Streaming video
Extended Real-Time Polling Service	For Variable Rate and delay dependent applications	VOIP with silence suppression
Non-real-time Polling Service	Variable rate and non-real time applications	FTP
Best Effort	Best Effort	E-mail, web traffic

A WSN module written for ns-2 is used to simulate real life situations and analyze the effect of various network conditions and load on QoS parameters. We have many QoS Parameters like Throughput, Average delay, Average Jitter etc. The effect of the service flow on the quality of service parameters such as throughput, average jitter and packet loss is studied.

II. Characteristics of WSN

The following are the characteristics of wireless sensor networks.

- **Dynamic topology**: Due to the node mobility, the topology of wireless sensor networks changes continuously and unpredictably. The link connectivity among the terminals of the network dynamically varies in an arbitrary manner and is based on the proximity of one node to another node. It is also subjected to frequent disconnection during node's mobility. WSNs should adapt to the traffic and propagation conditions as well as to the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the WSNs may not only operate within the network, but may require access to a public fixed network.

- **Bandwidth:** WSNs have significantly lower bandwidth capacity in comparison with fixed networks. The used air interface has higher bit error rates, which aggravates the expected link quality. Current technologies suitable for the realization of WSNs are IEEE 802.11(b,a) with bandwidth up to 54Mbps and Bluetooth providing bandwidth of 1Mbps. The nature of high bit-error rates of wireless connection might be more profound in WSNs. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subjected to noise, fading and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the links themselves can be heterogeneous.

- **Energy:** All mobile devices will get their energy from batteries, which is a scarce resource. Therefore the energy conservation plays an important role in WSNs. This important resource has to be used very efficiently. One of the most important system design criteria for optimization may be energy conservation.

- **Security:** The nodes and the information in WSNs are exposed to the same threats like in other networks. Additionally to these classical threats, in WSNs there are special threats, e.g. denial of service attacks. Also mobility implies higher security risks than static operations because portable devices may be stolen or their traffic may insecurely cross wireless links. Eavesdropping, spoofing and denial of service attacks should be considered.

- **Autonomous:** No centralized administration entity is required to manage the operation of the

different mobile nodes. In WSNs, each mobile terminal is an autonomous node, which may function as both a host and a router. So usually endpoints and switches are indistinguishable in WSNs.

- **Distributed Operation**: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a WSNs should collaborate among themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

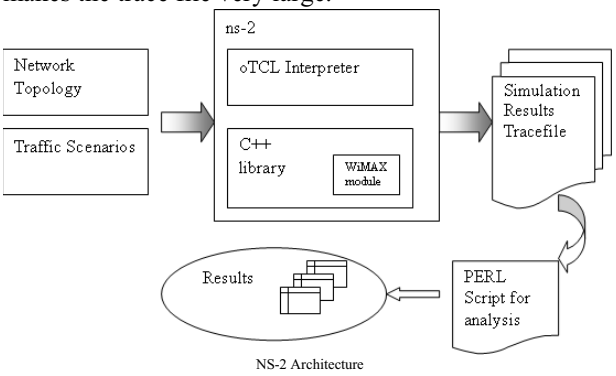
- **Multi-hop Routing:** Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop WSNs is simple in comparison with multi-hop WSNs in terms of structures and implementation. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

- **Light-Weight Terminals:** In most cases, the WSNs nodes are mobile devices with less CPU processing capability, small memory size and low power storage.

- **Infrastructure less and Self Operated:** A wireless sensor a network includes several advantages over traditional wireless networks, including: ease of deployment, speed of deployment and decreased dependence on a fixed infrastructure. WSN is attractive because it provides an instant network formation without the presence of fixed base stations and system administrators.

III. Network Simulator

The network simulator 2 (ns-2) is a popular tool for the simulation of packet-switched networks. It provides substantial support for simulation of TCP, routing, and MAC protocols over wired and wireless networks. The simulator core is written in C++. It has an OTcl (Object Tool Command Language) interpreter shell as the user interface and allows input models written as Tcl (Tool Command Language) scripts to be executed. Most network elements in ns-2 simulator are developed as classes, in object-oriented fashion. It is freely distributed and all the source code is available.
Figure shows basic structure of ns-2. The network topology and traffic agents etc are specified in the TCL file. It is parsed by the oTCL interpreter. The C++ library has all the implementation details. When ns-2 is run, the resulting data could be obtained in a trace file format. The trace file contains time stamp and information about each packet that is sent, received or dropped. It also has information about the packet size, type of packet etc. A base station and a subscriber station can be set up as a node in ns-2. As the number of nodes in the simulation increase, the packets that are sent and received increases. This makes the trace file very large.



NS-2 Architecture

IV. Performance Metrics

Performance Metrics encompasses Quality of Service to the end user in terms of several generic parameters. The perceived quality of service can be quantitatively measured in terms of several parameters. In the analysis, the throughput, average delay, average jitter, packet loss, end-to-end delay, Packet delivery fraction and energy were considered.

Throughput

Throughput is a measure of the date rate (bits per second) generated by the application. Equation shows the calculation for throughput TP, where PacketSize is the packet size of the ith packet reaching the destination, PacketStart is the time when the first packet left the source and PacketArrival is the time when the last packet arrived.

$$TP = \sum PacketSize / (PacketArrival - PacketStart)$$

From the trace file, based on the packet ID, each data packet was kept track of. The time a packet is sent, the time when the packet was received and the packet size was stored for all packets that reached the destination. To calculate throughput, the size of each packet was added. This gave the total data that was transferred.
The total time was calculated as the difference between the time the first packet started and the time the last packet reached the destination. Thus throughput is equal to the total data transferred

divided by the total time it took for the transfer.

Average Delay

Delay or latency would be time taken by the packets to transverse from the source to the destination. The main sources of delay can be further categorized into: source- processing delay, propagation delay, network delay and destination processing delay. Equation 2 show the calculation for Average Delay, where $PacketArrival_i$ is the time when packet "i" reaches the destination and $PacketStart_i$ is the time when packet "i" leaves the source. "n" is the total number of packets.

Average delay= (Packet Arrival- Packet Start)/n

Average Jitter

Delay variation is the variation in the delay introduced by the components along the communication path. It is the variation in the time between packets arriving. Jitter is commonly used as an indicator of consistency and stability of a network. Measuring jitter is critical element to determining the performance of network and the QoS the network offers.

Average Jitter= ((Packet Arrival+1)- (Packet Start+1))- ((Packet Arrival)-(Packet Start))/n-1

Packet loss or corruption rate

Packet loss affects the perceived quality of the application. Several causes of packet loss or corruption would be bit errors in an erroneous wireless network or insufficient buffers due to network congestion when the channel becomes overloaded.

Packet Loss= (∑(Lost Packet Size/∑Packet Size)*100

Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources is known as packet delivery fraction.

End-to-End Delay

Network delay is the total latency experienced by a packet to traverse the network from the source to the destination. At the network layer, the end-to-end packet latency is the sum of processing delay, packet, transmission delay, queuing delay and propagation delay. The end-to-end delay of a path is the sum of the node delay at each node plus the link delay at each link on the path.

Energy

The total number of energy consumed for packets transmitted and packet receiving during the simulation.

CONCLUSION

In this paper, the characteristics and service classes of wireless sensor networks were studied. We have concentrated here different performance metrics like PDF, end to end delay, energy, throughput, packet loss etc.

REFERENCES

[1] Performance Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model" International Journal of Computer Sciences, Vol 7, Issue 3, May 2010.

[2] B.Chen, K.Jamieson, H.Balakrishnan, and R.Morris. "Span : An energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks *in Pro of the ACM/ IEEE International Conference on Mobile Computing and Networking, July 2001.*

[3] Performance Measurement of various Routing Protocols in Adhoc Network" International Multiconference of Engineers and computer scientists 2009 Vol 1, March 2009.

[4] Study on Energy Conservation in MANET" journal of networks, vol 5, No 6, JUNE 2010.

[5] Performance Comparison Of Manet Protocols"©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 1.