An Analytical Study of the QOS Parameters of Routing of Protocols in a Wireless Sensor Network

Amanjeet Kaur, Anuj Gupta

Abstract: Wireless Sensor Network is a field where a lot of protocols are working already for the better optimization of the Wireless Network. The performance analysis is done on the basis of few parameters all together called Quality of service. This paper focuses on the analysis and understanding of the quality of service parameters and a brief description of the GA routing protocols to be used in this extension. This paper also focuses on the brief service review of the genetic algorithm based on the kind of services they can provide.

Index Terms: Genetic Algorithm, Protocols, Quality of Service, Routing Wireless Senor Network.

I. INTRODUCTION

Wireless Sensor network is a communications network made up of radio nodes organized in a sensor topology. Wireless sensor networks often consist of sensor clients, sensor routers and gateways. The sensor clients are often laptops, cell phones and other wireless devices while the sensor routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a sensor cloud. Access to this sensor cloud is dependent on the radio nodes working in harmony with each other to create a radio networks. A sensor network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. The animation below illustrates how wireless sensor networks can self form and self heal.
Wireless sensor networks can be implemented with various wireless technology including 802.11, 802.15, 802.16,[2] cellular technologies or combinations of more than one type. Sensor networking (topology) is a type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes, that is, it must collaborate to propagate the data in the network.
A Wireless Sensor network can be seen as a special type of wireless sensor networks. A Wireless Sensor network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. An ad-ho networks, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. The sensor routers may be mobile, and be moved according to specific demands arising in the network.
[1] Often the sensor routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the Wireless Sensor network differs from an ad-hoc network, since these nodes are often constrained by resources.

Manuscript received November, 2013.
Amanjeet Kaur, M-TECH (CSE) RIMT-IET , Mandi Gobindgarh Punjab, India.
Anuj Gupta, HOD (CSE) RIMT –IET Mandi - Gobindgarh Punjab, India.

Wireless sensor architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area. Wireless sensor architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Sensor architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing [3]. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area. The concept of wireless sensor networks is based on a simple equation [4]:
Sensing + CPU + Radio = Thousands of potential applications

II. QUALITY OF SERVICE OR SYSTEM EVALUATION MATRIX

A. System Evaluation Metrics

Now that we have established the set of application scenarios that we are addressing, we explore the evaluation metrics that will be used to evaluate a wireless sensor network. To do this we keep in mind the high-level objectives of the network deployment, the intended usage of the network, and the key advantages of wireless sensor networks over existing technologies. The key evaluation metrics for wireless sensor 18 networks are lifetime, coverage, cost and ease of deployment, response time, temporal accuracy, security, and effective sample rate. Their importance is discussed below.

B. Lifetime

Critical to any Wireless Sensor network deployment is the expected lifetime. The goal of both the environmental monitoring and security application scenarios is to have Nodes placed out in the field, unattended, for months or years. The primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. In many deployments it is not the average node lifetime19that is important, but rather the minimum node lifetime. In the case of wireless security systems, every node must last for multiple years. [5]

C. Coverage

Next to lifetime, coverage is the primary evaluation metric for a wireless network. It is always advantageous to have the ability to deploy a network over a larger physical area. This can significantly increase a system's value to the end user. It is important to keep in mind that the coverage of the network is not equal to the range of the wireless communication links being used.

Multi-hop communication techniques can extend the coverage of the network well beyond the range of the radio technology alone. In theory they have the ability to extend network range indefinitely? However, for a given transmission range, multi-hop networking protocols increase the power consumption of the nodes, which may decrease the network lifetime. Additionally, they require a minimal node density, which may increase the deployment cost.[6]

D. Cost and ease of deployment

A key advantage of wireless sensor networks is their ease of deployment. Biologists and construction workers installing networks cannot be expected to understand the underlying networking and communication mechanisms at work inside the wireless network. For system deployments to be successful, the Wireless Sensor network must configure itself. It must be possible for nodes to be placed throughout the environment by an untrained person and have the system simply work. Ideally, the system would automatically configure itself for any possible physical node placement. However, real systems must place constraints on actual node placements – it is not possible to have nodes with infinite range. The Wireless Sensor network must be capable of providing feedback as to when these constraints are violated.

The network should be able to assess quality of the network deployment and indicate any potential problems. This translates to requiring that each device be capable of performing link discovery and determining link quality .In addition to an initial configuration phase, the system must also adapt to changing environmental conditions. Throughout the lifetime of a deployment, nodes maybe relocated or large physical objects may be placed so that they interfere with the communication between two nodes. The network should be able to automatically reconfigure on demand in order to tolerate these occurrences. The initial deployment and configuration is only the first step in the network lifecycle. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost. The security application scenario in particular requires that the system be extremely robust. In addition to extensive hardware and software testing prior to deployment, the sensor system must be constructed so that it is capable of performing continual self-maintenance. When necessary, it should also be able to generate requests[7] when external maintenance is required. In a real deployment, a fraction of the total energy budget must be dedicated to system maintenance and verification. The generation of diagnostic and reconfiguration traffic reduces the network lifetime. It can also decrease the effective sample rate.

E. Response Time

Particularly in our alarm application scenario, system response time is a critical performance metric. An alarm must be signaled immediately when an intrusion is detected. Despite low power operation, nodes must be capable of having immediate, high-priority messages communicated across the network as quickly as possible. While these events will be infrequent, they may occur at any time without notice. Response time is also critical when environmental monitoring is used to control factory machines and equipment. Many users envision wireless sensor networks as useful tools for industrial process control. These systems would only be practical if response time guarantees could be met. The ability to have low response time conflicts with many of the techniques used to increase network lifetime. Network lifetime can be increased by having nodes only operate their radios for brief periods of time. If a node only turns on its radio once per minute to transmit and receive data, it would be impossible to meet the application requirements for response time of a security system. Response time can be improved by including nodes that are powered all the time. These nodes can listen for the alarm messages and forward them down a routing backbone when necessary. This, however, reduces the ease of deployment for the system.[8]

F. Temporal Accuracy

In environmental and tracking applications, samples from multiple nodes must be cross-correlated in time in order to determine the nature of phenomenon being measured. The necessary accuracy of this correlation mechanism will depend on the rate of23propagation of the phenomenon being measured. In the case of determining the average temperature of a building, samples must only be correlated to within seconds. However, to determine how a building reacts to a seismic event, millisecond accuracy is required. To achieve temporal accuracy, a network must be capable of constructing and maintaining a global time base that can be used to chronologically order samples and events. In a distributed system, energy must be expended to maintain this distributed clock. Time synchronization information must be continually communicated between nodes. The frequency of the synchronization messages is dependent on the desired accuracy of the time clock. The bottom line is maintenance of a distributed time base requires both power and bandwidth.

G. Security

Despite the seemingly harmless nature of simple temperature and light information from an environmental monitoring application, keeping this information secure can be extremely important. Significant patterns of building use and activity can be easily extracted from a trace of temperature and light activity in an office building. In the wrong hands, this information can be exploited to plan a strategic or physical attack on a company. Wireless sensor networks must be capable of keeping the information they are collecting private from eavesdropping. As we consider security oriented applications, data security becomes even more significant. Not only must the system maintain privacy, it must also be able to authenticate data communication. It should not be possible to introduce a false alarm message or to replay an old alarm message as a current one. A combination of privacy24 and authentication is required to address the needs of all three scenarios. Additionally, it should not be possible to prevent proper operation by interfering with transmitted signals. Use of encryption and cryptographic authentication costs both power and network bandwidth. Extra computation must be performed to encrypt and decrypt data and extra authentication bits must be transmitted with each packet.

This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime. Effective Sample Rate In a data collection network, effective sample rate is a primary application performance metric. We define the effective sample rate as the sample rate that sensor data can be taken at each individual sensor and communicated to a collection point in a data collection network. Fortunately, environmental data collection applications typically only demand sampling rates of 1-2 samples per minute. However, in addition to the sample rate of a single sensor, we must also consider the impact of the multi-hop networking architectures on a nodes ability to effectively relay the data of surrounding nodes. In a data collection tree, a node must handle the data of all of its descendents. If each child transmits a single sensor reading and a node has a total of 60 descendants, then it will be forced to transmit 60 times as much data.[7]

III. METHODS FOR MANAGING TRAFFIC

A. Traffic shaping

B. Traffic policing

These methods are often necessary on the edge separating a customer's network from a provider's network. Providers often force the customer to adhere to a specific policy service (or committed rate).This policy is referred to as the Service Level Agreement (SLA) between the customer and provider. Shaping and policing mechanisms differ in how each handles violations of the SLA. Shaping is usually implemented on the customer side, and will buffer traffic that exceeds the provider's committed rate. Thus, shaping can slow the traffic rate and siphon out traffic in compliance with the provider's SLA. Buffering traffic will often create delay and jitter, which can negatively impact sensitive traffic types. Shaping also requires sufficient memory to queue buffered traffic. Shaping provides no mechanism to re-mark traffic that exceeds the committed rate. Policing is usually implemented on the provider side, and will either drop or re-mark traffic that exceeds the provider's committed rate

•*Time Interval (TC)* – identifies the time interval for each burst, measured in seconds or sometimes milliseconds.

The CIR is calculated using the formula:

CIR (bps) = BC (bits) / TC (seconds)

With a token bucket system, the bucket is filled with tokens, and each token represents one byte. Thus, to transmit a 50-byte packet, the bucket must contain a minimum of 50 tokens. Tokens are consumed as traffic is transferred, and the bucket is refilled with tokens at the speed of the CIR. If the bucket is full, then excess tokens will spill out and are wasted. The capacity of the bucket is defined by the burst rate.

- *Generic Traffic Shaping (GTS)*: It implements shaping on a per-interface basis using the traffic-shape command.
- *Class-Based Shaping*: It implements shaping on a per-class basis using the shape command within a MQC policy-map.
- *Distributed Traffic Shaping (DTS)* : It offloads traffic shaping from the router processor to Versatile Interface Processors (VIPs). DTS is only available on high-end Cisco platforms.
- *Frame Relay Traffic Shaping (FRTS)*:It implements Frame-Relay specific shaping mechanisms, such as BECN or FECN.FRTS is only available on a Frame-Relay interface or sub interface, and is covered extensively in the Frame-Relay guide.

IV.ROUTING PROTOCOLS

Routing algorithms can be differentiated based on several key characteristics. First, the particular goals of the algorithm designer affect the operation of the resulting routing protocol. Second, various types of routing algorithms exist, and each algorithm has a different impact on network and router resources. Finally, routing algorithms use a variety of metrics that affect calculation of optimal routes. The following sections analyze these routing algorithm attributes.

V. DESIGN GOALS

Routing algorithms often have one or more of the following design goals:

- Optimality
- Simplicity and low overhead
- Robustness and stability
- Rapid convergence
- Flexibility

VI.GENETIC ALGORITHM

Genetic algorithms were formally introduced in the United States in the 1970s by John Holland at University of Michigan. The continuing price/performance improvement of computational system has made them attractive for some types of optimization. In particular, genetic algorithms work very well on mixed (continuous and discrete), combinatorial problems. They are less susceptible to getting 'stuck' at local optima than gradient search methods. But they tend to be computationally expensive. The key components of genetic algorithm are:

A) Mutation
B) Cross Over
C) Objective Function
D) Fitness Function

REFERENCES

1. Ali Chamam, and Samuel Pierre,"On the Planning of Wireless Sensor Networks: Energy-Efficient Clustering under the Joint Routing and Coverage Constraint", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 8, august 2009.
2. Jihene Rezgui, Abdelhakim Hafid and Michel Gendreau, "Distribute Admission Control in Mesh Network: Models, Algorithms, and Evaluation", IEEE transaction on vehicular technology, vol.59, no.3, march 2010
3. Gordon l.Stuber, Johan Barry, "Broadband MIMO-OFDM Wireless Communications".
4. Ming Jiang, and Lajos Hanzo, "Multiuser MIMO-OFDM for Next-Generation Wireless Systems", Proceedings of the IEEE | Vol. 95, No. 7, July 2007
5. Giuseppe Campobello1, Alessandro Leonardi and Sergio Palazzo, "Energy saving and Reliability in Wireless Sensor Networks Using a CRT-based Packet Splitting Algorithm", in 2002.
6. Giuseppe Anastasi, Marco Conti and Mario Di Francesco, "Energy Conservation in Wireless Sensor Networks: a Survey" ,University of Pisa, Italy National Research Council (CNR), Italy.
7. Dr. Jayakumari.J, " MIMO-OFDM for 4G Wireless Systems", International Journal of Engineering Science and Technology Vol. 2(7), 2010, 2886-2889.
8. A.Sharmila and Srigitha S.Nath, " Performance of MIMO Multi - Carrier CDMA with BPSK Modulation in Rayleigh Channel", International Conference and control Engineering (ICCCE 2012),12 & 13 April,2012.
9. Lizhong Zheng, David N. C. Tse , "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels" "IEEE transactions on information theory, vol. 49, no. 5, may 2003"