ANALYSIS OF CONCEPTS OF WIRELESS SENSOR NETWORKS

Samuel Madauda and Paluku Kazimoto
Faculty of Business, University of Arusha, United Republic of Tanzania

Abstract

Groups of specialized people and companies with a high-developed communications infrastructure intended to monitor and record conditions at diverse locations of their business to get up-to-date feedback. It is challenging for creating robust and reliable wireless sensor networks (WSNs). In this paper, we present an analysis of wireless network sensor demands and environment. It was demonstrated that wireless sensor networks well designed provides accurate feedback for attacks and that the current signal form in the appliance cable could accurately be reproduced with particular design. This leads to certain privacy issues and if the voltage values are sampled at even a higher rate, then a more accurate picture of information can be produced. This is a concern because of the inherent security issues encompassing wireless sensor networks. Large number of environmental applications makes use of wireless sensor networks that are deployed for many purposes to detecting attacks in different situations and provide feedback. However, WSNs need a well designed topology whereby large number of nodes require the presence of many contexts of similar nature where the same technology/application can be deployed as per topology considering buildings, humans, vehicles and all contexts that may exist in the current world in large numbers and as such representing huge potential markets for WSNs. From the results it is recommended that a study is needed to find out the contribution of WSNs to the security of nationals, properties, infrastructures and environment for country economic development.

Key words: Wireless, Sensor network, bandwidth and topologies.

Introduction

Groups of specialized people and companies with a high-developed communications infrastructure intended to monitor and record conditions at diverse locations of their business to get up-to-date feedback. Commonly monitored parameters may involve temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels, car key parking, and vital body functions. These show that sensor network consists of multiple detection stations that are called sensor nodes, which may be portable. And observing the nodes, every sensor node is equipped with a transducer, microcomputer, transceiver and power source.

A Wireless Sensor Networks (WSN) is a set of thousands of micro sensor nodes that have capabilities of sensing, establishing wireless communication between each other and doing computational and processing operations (Almazaydeh, Abdelfattah, Al-Bzoor, and Al- Rahayfeh, 2010). Since a wireless sensor network is a distributed real-time system. A wireless sensor network is a collection of nodes organized into a cooperative network.

The transducer generates electrical signals based on sensed physical effects and phenomena to determine the ultrasound image quality. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from a battery. Transducer is a device that produces sound waves that bounce off body tissues and make echoes. The transducer also receives the echoes and sends them to a computer that uses them to create a picture called a sonogram. Transducers (probes) come in different shapes and sizes for use in making pictures of different parts of the body (http://www.cancer.gov/dictionary?cdrid=367430)

The development of wireless sensor networks offers the promise of a flexible, low cost solution for monitoring critical infrastructure for traffic monitoring, personnel monitoring, operations and security monitoring. Although, there is installation of such system for monitoring the organization’s activities, sensor network has been proved more reliable in monitoring services as it is observed when a people
enter in certain offices that deal with security and high discretions of a country whereby no name may no be provided in this paper.

Wireless micro sensor networks have been identified as one of the most important technologies for the 21st century. Technology trends that impact the development of sensor networks are reviewed, and new applications such as infrastructure security, habitat monitoring, and traffic control are presented. Technical challenges in sensor network development include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. Wireless Sensor Networks have emerged as a new research technology in the distributed computing environment and plays a very important role in the pervasive computing to support various applications. It has a great potential to be utilized in battlefields and in different commercial applications like traffic surveillance, habitat monitoring, construction structures, smart homes, offices and many more (Chong and Kumar, 2003).

This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces. Since a wireless sensor network is a distributed real-time system a natural question is how many solutions from distributed and real-time systems can be used in these new systems? Unfortunately, very little prior work can be applied and new solutions are necessary in all areas of the system. Stankovic (2006) demonstrated that most past distributed systems research has assumed that the systems are wired, have unlimited power, are not real-time, have user interfaces such as screens and mice, have a fixed set of resources, treat each node in the system as very important and are location independent. In contrast, for wireless sensor networks, the systems are wireless, have scarce power, are real-time, utilize sensors and actuators as interfaces, have dynamically changing sets of resources, aggregate behavior is important and location is critical. Many wireless sensor networks also utilize minimal capacity devices, which places a further strain on the ability to use past solutions.

Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere. In such applications, running wires or cabling is usually impractical. A sensor network is required that is fast and easy to install and maintain (Lewis, 2004).

Sensor Networking Demands and bandwidth

The applications for wireless networks, because of bandwidth restrictions, uncertain deployment environments, and dynamic configuration demands present several technical challenges and requirements. For example, the networks must be autonomously reconfigurable, meaning that each node, after deployment, must be aware of, identify, and locate its neighbor nodes.

Teng and Zhang (2011) in their study indicated that demand localized and information retrieved with sensor networks, awareness of a user query’s content is displayed. In this scheme, a query’s name is resolved into the IDs and locations of corresponding sensor nodes before being distributed to the network. According to the location of sensor nodes, query distribution and data collection are performed in a corresponding local area. The query message is efficiently unicasted to the sink proxy in a query area, and is then forwarded to a localized area of the network. Sensing data are collected at a sink proxy, at which data are aggregated and sent to the sink node. Further, they agreed that since on-demand information retrieval may introduce intermittent and spatial data collections, the construction and maintenance of conventional aggregation structures such as clusters and chains will be at high cost.

Bennett, Wicker, and Cardell. (n.d) demonstrated that the sensor well design provides accurate root mean square values similar to those measured by digital multimeters. In addition to this there have also been able to show that the current waveform in the appliance cord could accurately be reproduced with particular design. This leads to certain privacy issues and if the voltage values are sampled at even a higher rate, then a more accurate picture of the customer’s power consumption can be created. This is a concern because of the inherent security issues encompassing wireless sensor networks.

Three techniques to manage wireless network bandwidth in sensor networks were described by Hull, Jamieson, and Balakrishnan (2003) who indicated that these techniques are tuned for a broad class on monitoring and control applications, where software running on general-purpose computers pull information from remote sensors and push actuations into the
network. They described that a simple rule-based approach to dynamically allocate bandwidth to sensor streams, a hop-by-hop flow control protocol to control congestion, and a load- and loss-sensitive sensor access point (SAP) selection protocol that improves the overall capacity of the sensor network.

Nowadays, both bandwidth allocation schemes and Bandwidth on Demand (BoD) schemes are widely adopted. Besides, in the modern Internet there is the tendency toward an even more distributed architectural approach. Actually, decentralized architectures are gaining more and more popularity. Peer to peer (p2p) applications and their communication paradigm are becoming popular. P2p networking allows obtaining a redundant architecture that reacts well against failure. Based upon p2p principles, this paper introduces a novel algorithm for configuring and managing bandwidth in a sensor network (Caviglione and Davoli, n.d.).

Bandwidth may raise restrictions; such a sensor network’s communications requirements may exceed its capacity. It may be seen from mobile agents, whereby data stay unprocessed at each local node, and the integration, processing or fusion code is transported to the data. Bandwidth may requirements may be reduced if the agent is smaller in size than the data. Under this assumption the network scales more efficiently, since the performance of the network is not affected by an increase in the sensor count.

**Sensor Network environments**

Environmental degradation and global warming are among the major global challenges facing sensor networks. These challenges include improving the efficient use of energy as well as climate change. Information Communication Technologies (ICT) and the Internet play a vital role in both, being part of the problem (they consume energy and are a source of pollution) and have the potential to provide important solutions to it (ICT applications in other sectors have major potential to improve environmental performance). Sensors and sensor networks have an important impact in meeting environmental challenges. Sensor applications in multiple fields such as smart power grids smart buildings and smart industrial process control significantly contribute to more efficient use of resources and thus a reduction of greenhouse gas emissions and other sources of pollution (OECD, 2009).

Large number of environmental applications makes use of wireless sensor networks. Sensor networks are deployed in forest to detect the origin of forest fires. Weather sensors are used in flood detection system to detect, predict and hence prevent floods. Sensor nodes are deployed in the environment for monitoring biodiversity (Khedo, Perseedoss and Mungur, 2010)

Sensor Networks have been found to be one of the most important technologies for 21st century. Wireless sensor network are gaining greater attention from the research community. Sensor node that is the basic element of wireless node network is composed of sensing computation and wireless communication unit. These sensor nodes are hence capable of observing physical phenomenon, process the observed and received information and communicate the observed or processed information to the nearby sensor nodes to form a network of sensor nodes called Wireless Sensor Networks. The wireless networking capability of the sensor enabled nodes have resulted in various interesting applications ranging from surveillance, smart homes, precision agriculture, disaster detection, and traffic control to vehicular and supply chain management application (Sharma, 2013).

The recent advances in Wireless Sensor Networks have given rise to many application areas in healthcare. It has produced new field of Wireless Body Area Networks. Using wearable and non-wearable sensor devices humans can be tracked and monitored. Monitoring from the healthcare perspective can be with or without the consent of the particular person. Even if it is with the consent of the person involved, certain social issues arise from this type of application scenario. The issues can be privacy, security, legal and other related issues. Healthcare sensor networks applications have a bright future and it is a must to take up these issues at the earliest. The issues should be carefully studied and understood or else they can pose serious problems. In this paper we try to raise and discuss these issues and find some answers to them (Al Ameen and Kwak, 2009).

Vellidis, et al. (2007) agued that although the wireless farm of the future offers great potential for improving efficiencies, it will not materialize without an equal quantum leap in the ability of farmers to understand electronics. Even the most robust wireless systems will require regular maintenance, repair and upgrades. As learnt from a decade of implementing precision agriculture, adding technology to the farm may reduce the number of people required but dramatically
increases the needed educational and competence level of the remaining workers. There will be a market for network and sensor specialists and other technologists in rural areas which may reverse the century-long trend of the brightest minds migrating from the countryside to the city. We are convinced that during the coming decade, wireless networks will offer the same type of quantum leap forward for farming that GPS provided during the past decade. Internet networks will eclipse all previous forms of distance communication and will provide the communications backbone for farms in the future.

Wireless Sensor Networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. The paper discusses about classification of WSN and challenges of the Next Generation WSN. One of the major challenges of Next Generation WSN is reduction of power consumption. The two approaches are discussed: Ultra-Low-Power Networks and Energy Harvesting. The paper also discusses about some major applications as designing low cost secured Intelligent Buildings, In-Home Health care and Agriculture (Srivastava, 2010).

Wireless Sensor Networks Topologies

For Wireless Sensor Networks (WSNs), sensor nodes have limited battery power and energy consumption is essential issue that needs attention on installation. Every sensor node can obtain its location information from other positioning system and send data to sink at any time. The characteristic of this is to divide WSN into network based on Topologies i.e. Bus, Tree, Star. Ring and Mesh Information of the position of nodes, and those nodes are organized within the network by the Topological way (Sharma, D., Verma, and Sharma, K., 2013).

The development of WSNs has taken traditional network topologies in new directions. Different some wireless sensor network topologies are demonstrated bellow:

Bus Topology: Bus network uses a multi-drop transmission medium, all node on the network share a common bus and thus share communication, and only one device can transmit at a time. It shown that a distributed access protocol of bus nodes determines which station is to transmit, data frames source and destination addresses, where each station monitors the bus and copies frames addressed to itself as shown in the figure bellow:

![Figure 1: Bus topology](image)

In this topology, there is a node that sends message to another node on the network that sends a broadcast message onto the network that all other nodes see, whereby only one intended recipient accepts and processes the message. Bus topology is easy to install but with more congestion of traffic and disadvantaged for a single path communication. However, bus networks work best with a limited number of nodes. If more than a few dozen nodes are added to a network bus, performance problems will likely result (Sharma, D., Verma, and Sharma, K., 2013). Bus topology is the most common type of interconnection networks since it can be implemented easily with a cheap hardware cost. A unique characteristic of a shared medium is its ability to support broadcast, in which all nodes on the medium can monitor network activities and receive the information transmitted on the shared medium (Narayana T, 2013).

Tree Topology: The network use a central hub called a root node as the main communication router. In sensor network path may be single hop or multi hop, sensor node for getting data sense into the environment and send them to the sink and sensor forwards them to its parent after receives data messages from its children. It is important to find an optimal shortest path tree with maximum lifetime and shorter delay but slightly high time complexity and but more suitable for distributed implementation (Sharma, D., Verma, and Sharma, K., 2013). The tree topology is essentially a hybrid of the bus and star layouts. This topology has a root node connected to a certain number of descendant nodes. Each of these nodes is in turn connected to a disjoint set of descendants. A node with no descendant is a leaf node. Bellow figure shows a tree topology. The biggest drawback of the tree topology as a general-purpose interconnection network is that the root and the nodes close to it become a bottleneck. Additionally, there are no alternative paths between any pair of nodes (Narayana T, 2013).
Star Topology: Star Network Topology requires the use of a central top-level node to which all other nodes are connected. Messages received by the top level node can either be broadcast to all subordinate nodes, or if the top level device is of high enough fidelity, sent only to the desired subordinate node. Inter node messaging delays are reduced with this configuration. Failure in the connection between the top level node and any subordinate node, or failure in a subordinate node will not disrupt the entire network and below is the design of star topology:

Ring Topology: For a ring network, every node has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either clockwise or counterclockwise). A failure in node breaks the loop and can take down the entire network, but congestion of traffic and double path communication (Sharma, D., Verma, and Sharma, K., 2013). Ring network connects computers in a circle of point-to-point connections, with no central server, such as a series of desktop computers in an office. Each node handles its own applications and also shares resources over the entire network. If one node becomes inoperative, the other nodes are still able to maintain contact with one another. Such a network is best for decentralized systems in which no priorities are required as shown below:

Mesh Topology: Mesh topologies involve messages can take any of several paths from source to destination. (Recall that even in a ring, although two paths exist, messages can only travel in one direction.) A mesh network in which every node connects to every other is called a full mesh and there is partial mesh networks also exist in which some devices (nodes) connect only indirectly to others (Sharma, D., Verma, and Sharma, K., 2013).

Mesh Network Topologies capitalize on path redundancy. This Topology is preferred when traffic volume between nodes is large. A proportion of nodes in this type of network have multiple paths to another destination node. With the exception of the Bi-directional Ring (and this was only when a failure was
detected) each of the topologies discussed so far had only one path from message source to message destination. Thus the probability of single point network failure is greatly minimized with Mesh Network Topology (Meador, 2008).

**Conclusion**

It is challenging for creating robust and reliable wireless sensor networks (WSNs). In this paper, we present an analysis of wireless network sensor demands and environment. It was demonstrated that wireless sensor networks well designed provides accurate feedback for attacks and that the current signal form in the appliance cable could accurately be reproduced with particular design. This leads to certain privacy issues and if the voltage values are sampled at even a higher rate, then a more accurate picture of information can be produced. This is a concern because of the inherent security issues encompassing wireless sensor networks. Large number of environmental applications makes use of wireless sensor networks that are deployed for many purposes to detecting attacks in different situations and provide feedback. However, WSNs need a well designed topology whereby large number of nodes require the presence of many contexts of similar nature where the same technology/application can be deployed as per topology considering buildings, humans, vehicles and all contexts that may exist in the current world in large numbers and as such representing huge potential markets for WSNs. Therefore, we recommend that a study is needed to find out the contribution of WSNs to the security of nationals, properties, infrastructures and environment for country economic development.

**References**


Endnotes

