A NEW EMERGING TECHNOLOGY: WIRELESS SENSOR NETWORK WITH PERSONAL NETWORK

Pankaj Dhumane[1] and Bharti Dikhit[2]

[1]Assistant Professor, Department of Computer Science, Sardar Patel Mahavidyalaya, Chandrapur
Email: pdhumane@rediffmail.com
[2] Lecturer, Department of Computer Application, Sardar Patel Mahavidyalaya, Chandrapur
Email: bharti.kurekar@gmail.com

ABSTRACT

Wireless sensor network (WSN)is an emerging technology that shows great promise for various applications. The inclusion of wireless communication technology incurs various types of security threats. Sensor nodes are typically smaller, less powerful, and more prone to failure than nodes in an ad hoc network. These differences indicate that protocols that are valid in the context of ad-hoc networks may not be directly applicable for sensor networks. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks and personal sensor network. We review several protocols like IEEE 802.15 and UPnP; they provide security in sensor networks, with an emphasis on privacy and security in WSN (longer range) and PSN (Shorter range).

***Keywords*:** WSN, PSN, UPnP

INTRODUCTION

Wireless Sensor Network

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollination at different locations. Typically sensors form a network using different radio interfaces based on the nature of deployment of WSN.

Personal Sensor Network in a sense is a miniature form of a WSN related to a person and activities of that person that are of interest from a monitoring and management viewpoint. typical PSN are monitoring vital signs for health ,monitoring home appliances, temperature ,automobiles ,using proximity sensor to ensure that people don`t lose their belongings etc. In this case the sensors are providing feedback to the person using the sensors. Also , a completely new set of services are possible because sensors around the person will provide many inputs in setting the context of person at the time, coupled the Internet that enables the person to share the data to other Nodes in the network that wish t o the data for adding more

value to person`s life. This document focuses on these aspects to describe various uses of such a network, the challenges there of for adaptation in real –world scenarios.

Internet and Mobile phone will greatly add values to the Personal Sensor Networks. Although sensors of all types have been available for a while, there was no computing device that a person could carry on him/her that would receive the data from various sensors and process the information. Ubiquitous Mobile Phone could now be the device that acts computing node and provide information to the person using the mobile through visual output/audio/vibration etc. Mobile phones of today have always on connectivity to the internet .This enables the sensor information (where applicable) to be shared the person`s social network also which provides enhances the context of the person. In some cases, sensor information can be transmitted to a centralized computing node over the internet that provides monitoring and necessary computing.

Wireless Sensor Network versus Personal Sensor Network

A typical WSN has a large network of sensors acquiring data or sending events of interests (triggers) over a large area to nodes that receive the data and perform the computing .The sensors are stationary .However, in the case of a PSN the person is mobile and so are the sensors. The objective of the sensors in the case to collect or trigger data related to the mobile person. Hence the network architectures, computing are very different. Ad-hoc networks are best suited for such scenarios.

Weakness of Personal Sensor Network

Limited Memory and Storage Space: A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

Power Limitation: Energy is the biggest constraint to wireless sensor capabilities .We assume that once sensor nodes are deployed in a sensor network ,they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensors node and the entire sensor network.

Reliable Transfer: Normally the packet-based routing of the sensor network is connectionless and thus they are unreliable because packets may get damaged due to channel errors or due to some other reasons. The result is lost or missing packets. Thus the unreliable wireless communication channel also results in damaged Architecture.

Why Privacy and Security is required for Personal Sensor Network?

Person may require the context will receive data from the sensor after appropriate permissions from the person of interest .Instead of disclosing the complete data that may be dangerous. In general, morphing of the actual data to another intermediate form before sending over Internet will be a requirement to protect the person from malicious use of the data.

Using GPS coordinates, it possible to accurately locate the person`s location or where the person is currently staying. This will impact privacy and security especially for young persons who are the most extensive users of Internet.

For privacy, user`s may not want to share their current location or pictures of the surroundings etc, where as they may be willing to share the weather information outside of the home.

Users may be willing to share sensitive data like location with family members, but not co-workers and other friends.

In case of sensor network, which typically is more sensitive like current interests, hobbies, users may not desire to share the information with everyone.

Sensor networks for collecting information and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to desire sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitant's private activities.

The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For examples, thieves can spread sensors on the grounds of a private home to detect the inhabitants `presence. If the sensors are small enough, they can also plant them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop.

Hence, a consistent way to define the sensor data, categorization and selective profiling to distribute the data is required.

What type of Security is required?

Detector must be able not only to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Such technologies might not prevent unauthorized parties from deploy eying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem somewhat.

In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously. Ensuring that sensed information stays within the sensor network and is accessible only to trusted parties is an essential step toward achieving privacy.

Another approach is to process queries in the sensor network in a distributed manner so that no single node can observe the query results in there. This approach guards against potential system abuse by compromised malicious nodes.

Security Issues in Wireless Sensor Networks

Data confidentiality

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks .In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers process, hence achieving confidentiality .since public key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

Privacy of Sensed Data

Sensor networks are tools for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants 'private activities.

The main privacy problem, however is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site surveillance .Rather; sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in alow-risk, anonymous manner, Remote access also allows a single adversary to monitor multiple sites simultaneously.

Denial of Service Attacks

As safety –critical applications use more sensor networks, the potential damage of operational disruptions becomes significant .Defending against denial –of –service attacks, which aim to destroy network functionality rather than subverting it or using the sensed information, is extremely difficult .DOS attacks can occur at the physical layer-for example, via radio jamming. They can also involve malicious transmissions into the network to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery exhaustion in sensor nodes—for example, by sending a sustained series of useless communications that the targeted nodes will expend energy processing and may also forward to other nodes. More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For example, they could create routing loops that will eventually exhaust all nodes in the loop.

Malicious Use of Wireless Sensor Network

The Proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purpose. For examples, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough , they can also plant them on computers and cell phones to extract private information and passwords .With widespread use, the cost and availability barrier that discourage such attacks will drop.

Universal Plug and Play

(UPnP) is one of popular sharing protocol shares with various electronic devices and it is a set of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. UPnP achieves this by defining and publishing UPnP device control protocols (DCP) built upon open, Internet –based communication standards.

Application of UPnP

The UPnP architecture supports zero- configuration networking and automatic discovery whereby a device can dynamically join a network .UPnP technology can run on many media that support IP including Ethernet. FireWire, IR (IrDA) ,home wiring and RF (Bluetooth. Wi-Fi) No special device driver support is necessary; common protocols are used. UPnP architecture enables devices to present a user interface through a web browser .Any operating system and any programming language can be used to build UPnP products(Java, Linux, Mac OS,and Windows)

Benefit of UPnP

UPnP can solve NAT (Network Address Translation) connection problems with active (PORT) mode.

THE client is behind a NAT and wants to connect to an FTP server supporting PORT mode only (because the server is behind a NAT as well or due to security/firewall policies). In this case without UPnP the ports have to be manually enabled and forwarded in the NAT router and a port range has to be defined in the FTP client configuration .With the new (UPnP) feature everything is automatically handled for the user.

Detect external IP address (Send correct IP address in PORT command) Dynamic Post Mappings (Add/Remove port mapping on the fly)

The Port are only opened as long as they`re needed. The UPnP mappings are automatically removed when the transfer is finished or aborted.

IEEE 802.15 and Bluetooth: WPAN Communications

IEEE 802.15, a standardization of Bluetooth wireless specification defined by IEEE, is for wireless personal area networks (WPANs). IEEE 802.15 has characters such as short –range, low power, low cost, small networks and communication of devices within a Personal Operating Space.

The initial version, IEEE 802.15 .1, was adapted from the Bluetooth specification and is fully compatible with Bluetooth 1.1 .The specification also allows for connection to the Internet 802.15.1/Bluetooth specifies standards in on the Physical layer and Data link layer of the OSI model with the following four sub-layers.

RF layer: The air interface is based on antenna power range starting from 0 dBm up to 20 dBm Bluetooth operates in the 2.4 GHz band and the link range is any-where from 10 centimeters to 10 meters.

Baseband layer: established the Bluetooth physical link between devices forming a PICO-net –a network of devices connected in an ad hoc fashion using Bluetooth technology.

Link Manager: sets up the link between Bluetooth devices. Other functions of the link manager include security, negotiation of baseband packet sizes, power mode and duty cycle control of the Bluetooth device, and the connection states of a Bluetooth device in a Pico net.

Architectural Overview

In most UPnP scenarios, a control Point controls the operation of one or more UPnP devices in order to accomplish the desired behavior. Although the Control Point is managing multiple devices, all interactions occurs in isolation between the Control Point and each device .the control Point coordinates the operation of each device to achieve an overall, synchronized, end-user effect. The individual devices do not interact directly with each another. All of the coordination between the devices is performed by the Control Point and not the devices themselves.

UPnP protocol and Sensor Network Management Architecture

Above showed figure represents sensor network management architecture based on the UPnP .this architecture is composed of three parts:UPnP Control Point ,Boss, and non UPnP sensor nodes.

In UPnP technology, the control Point is the entity in the network that works with the services provided by UPnP devices. In our architecture, the control point is a device to control and manage a sensor network using the services provided by UPnP proxy (Bridge of the Sensors) that has enough powerful resources to computed UpnP protocol .This base node uses bridge architecture for communication between the sensor network and control point .Finally ,each sensor node is a non UPnP device which has sensing capabilities . But the current sensor device does not have sufficient resources to be able to process the UPnP protocol. In our architecture, the control point and BOSS communicate with each other using UPnP protocol .On the other hand, non UPnP sensor devices and BOSS use network specific protocol for communication.

CONCLUSION

For short range and low power wireless (less than 10 meters) communications among personal devices such as PDA, Bluetooth and sequent IEEE standards (802.15) are taking effects. For long range wireless communication in the metropolitan areas, Wi-max as defined in the IEEE 802.16 is the standard but UPnP protocol is suited for lower range and long range and application and benefits of UPnP protocol are already discussed.

REFERENCES

1. Wireless Sensor Network By Kazem Sohraby ,Daniel minoli,Taieb.
2. Cryptography and network security-By William Stallings.
3. Mobile Communications –By Jochen Schiller
4. Mobile and wireless Design Essentials –By Martyn Mallick.
5. Security in wireless Sensor networks Published in August 2008 IEEE Explore.
6. http:// network security .com