IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Wireless Sensor Network Security and Analysis

G. Anuradha

Assistant Professor, Department of Computer Science, A.V.C. College (Autonomous), Mannampandal

Abstract: A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, and cost, hardware, and system constraints. The sensor nodes will perform significant signal processing, computation, and network self-configuration to achieve scalable, robust and long-lived networks.. More specifically, sensor nodes will do local processing to reduce communications, and consequently, energy costs. We believe that most efficient and adaptiverouting model for WSN is cluster based hierarchical model. For a cluster based sensor network,the cluster formation plays a key factor to the cost reduction, where cost refers to the expense ofsetup and maintenance of the sensor networks. In this paper, we will take a more security in WSN and discuss countermeasures. The goal of our survey is to present a comprehensive review of the recent literature since the publication of [I.F. Akyildiz, W. Su, and Y. Sankarasubramaniam. Cayirci, A survey on sensor networks, IEEE Communications Magazine, 2002]. Following a top-down approach, we give an overview of several new applications and thenreview the literature on various aspects of WSNs. We classify the problems into three differentcategories: (1) internal platform and underlying operating system, (2) communicationprotocol stack, and (3) network services.

Keywords: Wireless sensor network (WSN), Network Security, Micro-Electro-Mechanical Systems (MEMS)

1. INTRODUCTION

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. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, a radio, and an actuator. A WSN typically has little or no infrastructure.

It consists of a number of sensor nodes (few tens to thousands) working together to monitor a region to obtain data about the environment.. WSNs have great potential for many applications in scenarios such as military target tracking and surveillance [2,3], natural disaster relief [4]

2. OVERVIEW OF KEY ISSUES

Current state-of-the-art sensor technology provides a solution to design and develop many types of wireless sensor applications.. To enable wireless sensor applications using sensor technologies, the range of tasks can be broadly classified into three groups . The first group is the system. Each sensor node is an individual system. In order to support different application software on a sensor system, development of new platforms, operating systems, and storage schemes are needed. The second group is communication protocols, which enable communication between the application and sensors. They also enable communication between the sensor nodes.

The last group is services which are developed to enhance the application and to improve system performance and network efficiency. As sensor nodes operate on limited battery power, energy usage is a very important concern in a WSN; and there has been significant research focus that revolves around harvesting and minimizing energy.. . In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area. In pre-planned deployment, there is grid placement, optimal placement 2-d and 3-d placement [8] [9]

3. WSN ARCHITECTURE

In a typical WSN we see following network components –
• Sensor motes (Field devices) – Field devices are mounted in the process and must becapable of routing packets on behalf of other devices. In most cases they characterize orcontrol the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009. Gateway or Access points – A Gateway enables communication between Host application and field devices.

• Network manager – A Network Manager is responsible for configuration of thenetwork, scheduling communication between devices (i.e., configuring super frames),management of the routing tables and monitoring

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

and reporting the health of thenetwork.• Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

4. WSN SECURITY ANALYSIS

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremelyvulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bitsin the channel, replay previously heard packets and many more. Securing the Wireless SensorNetwork needs to make the network support all security properties: confidentiality, integrity,authenticity and availability. Attackers may deploy a few malicious nodes with similar hardwarecapabilities as the legitimate nodes that might collude to attack the system cooperatively.

Theattacker may come upon these malicious nodes by purchasing them separately, or by "turning" afew legitimate nodes by capturing them and physically overwriting their memory. Also, insome cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversarycompromises a node, she can extract all key material, data, and code stored on that node. Whiletamper resistance might be a viable defense for physical node compromise for some networks,we do not see it as a general purpose solution. Extremely effective tamper resistance tends toadd significant per-unit cost, and sensor nodes are intended to be very inexpensive [5] [6] [7]

5. INTERNAL SENSOR SYSTEM

For a sensor to operate in a wireless sensor network,there are several internal system issues that need to be addressedthrough the system platform and operating system(OS) support. In addition, supporting standards, storage, and physical test beds are reviewed in the following subsections.

5.1. System platform and OS support

Current WSN platforms are built to support a widerange of sensors. Products that offer sensors and sensor nodes have different radio components, processors, andstorage. It is a challenge to integrate multiple sensors ona WSN platform since sensor hardware is different andprocessing raw data can be a problem with limited resourcesin the sensor node. System software such as theOS must be designed to support these sensor platforms.Research in this area involves designing platforms thatsupport automatic management, optimizing network longevity,and distributed programming.

Below we discusstwo platforms: a Bluetooth-based sensor system anda detection-and-classification system, Bluetooth-based sensor networks reported a study todetermine if a Bluetooth-based sensor node is viable for aWSN. Typical radio components used in a WSN are basedon fixed frequencies where sensor nodes within communicationrange compete for a shared channel to transmitdata. But Bluetooth is based on spread-spectrum transmissionwhere separate channels are used to transmit data.The Bluetooth-based devices used in the experiments are BT nodes developed by ETH Zurich [36].

A stripped down version of the Bluetooth stack for Tiny OS was designed and ported into the BT nodes. In order to support amulti-hop network, each BT node is equipped with two radios: one configured to operate as a master and the otheras a slave.

The master radio can support up to seven connectionswhile the slave radio looks for another node to connectto. Because Bluetooth is connection oriented, a master andslave connection must be established before data is exchanged.When a new node joins the network, its slave radiois first enabled.

The new node tries to connect itself with the rest of the network. When the new node finds a node to connectto as its slave, it turns on the master radio to acceptconnections from nodes that are not yet connected to thenetwork.

6. COMMUNICATION PROTOCOL

The development of a reliable and energy-efficient protocolstack is important for supporting various WSN applications.Depending on the application, a network mayconsist of hundreds to thousands of nodes. Each sensor nodeuses the protocol stack to communicate with one anotherand to the sink.

Hence, the protocol stack must be energyefficient in terms of communication and be able to workefficiently across multiple sensor nodes. We review the variousenergy-efficient protocols proposed for the transportlayer, network layer, and data-link layer, and their cross layer inter actions in the following subsections. Transport layer

The transport layer ensures the reliability and quality ofdata at the source and the sink. Transport layer protocols inWSNs should support multiple applications, variable reliability, packet-loss recovery, and congestion control mechanism.The development of a transport layer protocolshould be generic and independent of the application. Itshould provide variable packet reliability for differentapplications.

Each WSN application can tolerate differentlevels of packet loss. Packet loss may be due to bad radio communication, congestion, packet collision, full memorycapacity, and node failures. Any packet loss can result inwasted energy and degraded quality of service (QoS) in data delivery. Detection of packet loss and correctly recoveringmissing packets can improve throughput and energyexpenditure.

DOI 10.17148/IJARCCE.2016.5928

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

7. NETWORK SERVICES

Sensor provisioning, management, and control servicesare developed to coordinate and manage sensor nodes.They enhance the overall performance of the network interms of power, task distribution, and resource usage. Provisioningproperly allocates resources such as power andbandwidth to maximize utilization. In provisioning, thereis coverage and localization. Coverage in a WSN needs toguarantee that the monitored region is completely coveredwith a high degree of reliability.

Coverage is important because it affects the number of sensors to be deployed, theplacement of these sensors, connectivity, and energy.

Localization is the process by which a sensor node triesto determine its own location after deployment. Managementand control services play a key role in WSNs as theyprovide support to middleware services such as security, synchronization, data compression and aggregation, cross-layer optimization, etc. In this section, we study provisioning, control, and management services based on theirobjectives.

A brief summary of each plane is described ineach of the sections below.LocalizationIn WSNs, sensor nodes that are deployed into the environmentin an ad hoc manner do not have prior knowledgeof their location. The problem of determining the node'slocation (position) is referred to as localization. Existinglocalization methods include global positioning system(GPS), beacon (or anchor) nodes, and proximity-basedlocalization.

Equipping the sensor nodes with a GPS receiveris a simple solution to the problem. However, such aGPS-based system may not work when the sensors are deployedin an environment with obstructions such as densefoliage areas. The beacon (anchor) method makes use ofbeacon (anchor) nodes, which know their own position,to help sensors determine their position.

This method hasits shortcoming. It does not scale well in large networksand problems may arise due to environmental conditions.Proximity-based localization makes use of neighbor nodes to determine their position and then act as beacons for other nodes. Below we review some of the key localizationtechniques that differ from the above methods.

Moore's algorithm: Ref. [13] presents a distributed localizationalgorithm for location estimation without the useof GPS or fixed beacon (anchor) nodes. A key feature of thisalgorithm is the use of a robust quadrilateral. A robustquadrilateral is a fully-connected quadrilateral whose foursub-triangles are robust. Localization based on robustquadrilateral can be adjusted to support noisy measurementsand it correctly localizes each node with a highprobability.

8. WHY NEED SECURITY(WSN)

Wireless sensor networks have many applications in military, homeland security and other areas..In that many sensor networks have mission –critical tasks. Security is critical for such networks deployed in hostile environments. Most sensor networks actively monitor their surroundings, and it is often to deduce information other than the data monitored.Such unwanted information leakage often results in privacy breaches of the people in environment.Moreover, the wireless communication employed by sensor Networks facilities eavesdropping and packet injection by an adversary.

The combination of these factors demands security for sensor networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments.Providing security in sensor networks is even more difficult than MANETS due to the resource limitations of sensor nodes.[12]

9. SECURITY REQUIREMENTS

- Confidentially
- Integrity
- Availability
- Freshness
- Additional requirements:

* Authentication
* Access-control
* Privacy
* Authorization
* Non-repudiation
* Survivability

10. TYPES OF SENSOR NETWORKS

Current WSNs are deployed on land, underground, and underwater. Depending on the environment, a sensor network faces different challenges and constraints. There are five types of WSNs: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, and mobile WSNTerrestrial WSNs. Typically consist of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area, either in an ad hoc or in a pre-planned manner. In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area.

Underground WSNs consist of a number of sensor nodes buried underground or in a cave or mine used to monitor underground conditions. Additional sink nodes are located above ground to relay information from the sensor nodes to the base station. An underground WSN is more expensive than a terrestrial WSN in terms of equipment, deployment, and maintenance. Underground sensor nodes are expensive because appropriate equipment parts must be selected to ensure reliable communication through soil, rocks, water, and other mineral contents.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Underwater WSNs[10] consist of a number of sensor nodes and vehicles deployed underwater. As opposite to terrestrial WSNs, underwater sensor nodes are more expensive and fewer sensor nodes are deployed.

Autonomous underwater vehicles are used for exploration or gathering data from sensor nodes. Compared to a dense deployment of sensor nodes in a terrestrial WSN, a sparse deployment of sensor nodes is placed underwater. Typical underwater wireless communications are established through transmission of acoustic waves.

Multi-media WSNs [11] have been proposed to enable monitoring and tracking of events in the form of multimedia such as video, audio, and imaging. Multi-media WSNs consist of a number of low cost sensor nodes equipped with cameras and microphones.

These sensor nodes interconnect with each other over a wireless connection for data retrieval, process, correlation, and compressionMobile WSNs consist of a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability sense, compute, and communicate like static nodes. A key difference is mobile nodes have the ability to reposition and organize itself in the networkApplications of wireless sensor network

Wireless sensor networks have gained considerable popularity due to their flexibility in solving problems in different application domains and have the potential to change our lives in many different ways.

WSNs have been successfully applied in various application domains (Akyildiz et al. 2002;Bharathidasan et al., 2001), (Yick et al., 2008; Boukerche, 2009), (Sohraby et al., 2007), and (Chiara et al., 2009;Verdone et al., 2008), such as:Military applications: Wireless sensor networks be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems. Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored.

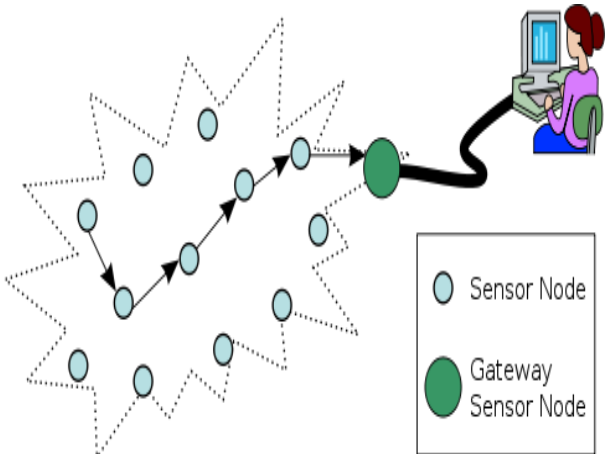
When the sensors detect the event being monitored (heat, pressure etc), the event is reported to one of the base stations, which then takes appropriate action.Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.

Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.

Features of WSN:

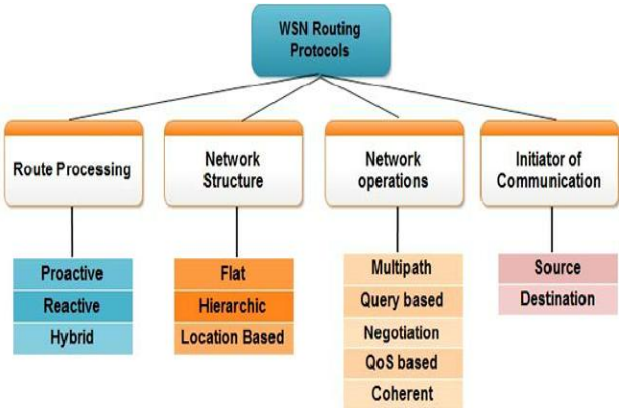
The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting.
- Ability to cope with node failures (resilience)
- Some mobility of nodes (for highly mobile nodes see MWSNs)
- Heterogeneity of nodes.
- Scalability to large scale of deployment.



APPENDIX

The following table shows the wireless sensor network routing protocols:



11. CONCLUSION

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. Inparticular, Wireless Sensor Network product in industry will not get acceptance unless there is afool proof security to the network. In this paper, we have made a threat analysis to the WirelessSensor Network and suggested some counter measures. Link layer encryption andauthentication mechanisms may be a reasonable first approximation for defense against moteclass outsiders, but cryptography is not enough to defend against laptop-class adversaries andinsiders: careful protocol design is needed as well. Security concerns constitute a potential stumbling block to the impending widw deployment of sensor networksWSNs

DOI 10.17148/IJARCCE.2016.5928

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

are still under development and many protocols designed so far for WSNs have not taken security into consideration. On the other hand the salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads..We summarize typical attacks on sensor networks and several important security issues relevant to the sensor networks, including key management, secure time synchronization, secure location discovery and etc., Many security issues in WSNs remain open and I expect to see more research activities on these exciting topics in the future.

REFERENCES

[1] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai, K. Frampton, Sensor network-based countersniper system, in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD, 2004.

[2] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005.

[3] M. Castillo-Effen, D.H. Quintela, R. Jordan, W. Westhoff, W. Moreno, Wireless sensor networks for flash-flood alerting, in: Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic, 2004.

[4] S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009

[5] D. Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008, 3 (1). International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009

[6] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008.

[7] B. Mukherjee, D. Ghosal, Placement of network services in sensor networks, Self-Organization Routing and Information, Integration in Wireless Sensor Networks (Special Issue) in International Journal of Wireless and Mobile Computing (IJWMC) 1 (2006) 101–112.

[8] D. Pompili, T. Melodia, I.F. Akyildiz, Deployment analysis in underwater acoustic wireless sensor networks, in: WUWNet, Los Angeles 2006.

[9] T. Melodia, Challenges for efficient communication in underwater acoustic sensor networks, ACM Sigbed Review 1 (2) (2004)

[10] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks Elsevier 51 (2007) 921–960.

[11] Chris karlof and davidwagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc networks, Elsevier publicaions, Vol.1,pp.293-315,2003.

[12] D. Moore, J. Leonard, D. Rus, S. Teller, Robust distributed network localization with noisy range measurements, in: Proceedings of the Sensys'04, San Diego, CA, 2004.

DOI 10.17148/IJARCCE.2016.5928