WIRELESS SENSOR NETWORKS ARCHITECTURE & SECURITY: A SURVEY

K. Helen Jessie Bala
Department of Computer Science
Bishop Caldwell College
Manonmaniam Sundaranar University
balachristo@gmail.com

S.Maria Packiam
Department of Information Technology
Bishop Caldwell College
Manonmaniam Sundaranar University
mariapacks@gmail.com

Abstract - Wireless sensor networks (WSN) are an emerging technology in recent years. A wireless network is a network that uses wireless data connections between network nodes. Wireless sensor network consists of small nodes with sensing, computation and wireless communication capability. In a WSN the architecture plays an important role. The design of WSN depends upon the application and its factors such as the environment, application's objectives, cost and system constrains. As the WSN continues to grow in many applications that deals with sensitive data and operates in hostile unattended environments in recent years, it is very must to focus in the security of the network. A wireless sensor network has important applications such as remote environmental and tracking. The security of the network is designed carefully from the beginning of the system design. However, due to unpredictable environmental changes and system constrains, the security in wireless sensor network faces many challenges than the traditional networks. This paper gives a survey of the types of WSN and the comparison between the types. Also the paper gives a survey on the obstacles and requirements in the sensor security.

I. INTRODUCTION

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. There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. Sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult since there are so many nodes. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner. The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions.

Sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defences even harder. With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks. We classify the main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. In this paper we are focusing on the types of WSNs, obstacles & requirements of a secure WSN.

II. TYPES OF SENSOR NETWORKS

Current WSNs are deployed on land, underground, and underwater. Depending on the environment, a sensor net- work faces different challenges and constraints. There are five types of WSNs: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, and mobile WSN

A. TERRESTRIAL WSNs

Terrestrial WSNs [1] 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. In pre-planned deployment, there is grid placement, optimal placement, 2-d and 3-d placement models. In a terrestrial WSN, reliable communication in a dense environment is very important. Terrestrial sensor nodes must be able to effectively communicate data back to the base station. While battery power is limited and may not be rechargeable, terrestrial sensor nodes however can be equipped with a secondary power source such as solar cells. In any case, it is important for sensor nodes to con-serve energy. For a terrestrial WSN, energy can be con-served with multi-hop optimal routing, short transmission range, in-network data aggregation, eliminating data redundancy, minimizing delays, and using low duty-cycle operations

B.UNDERGROUND WSNs

Underground WSNs [2, 3] 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. The underground environment makes wireless communication a challenge due to signal losses and high levels of attenuation. Unlike terrestrial WSNs, the deployment of an underground WSN requires careful planning and energy and cost considerations. Energy is an important concern in underground WSNs. Like terrestrial WSN, underground sensor nodes are equipped with a limited battery power and once deployed into the ground, it is difficult to recharge or replace a sensor node's battery. As before, a key objective is to

conserve energy in order to increase the lifetime of network which can be achieved by implementing efficient communication protocol

C. UNDERWATER WSNs

Underwater WSNs [4,5] 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. A challenge in underwater acoustic communication is the limited bandwidth, long propagation delay, and signal fading issue. Another challenge is sensor node failure due to environmental conditions. Underwater sensor nodes must be able to self-configure and adapt to harsh ocean environment. Underwater sensor nodes are equipped with a limited battery which cannot be replaced or recharged. The issue of energy conservation for underwater WSNs involves developing efficient underwater communication and net- working techniques.

D. MULTI-MEDIA WSNs

Multi-media WSNs [6] 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 compression. Multi-media sensor nodes are deployed in a pre-planned manner into the environment to guarantee coverage. Challenges in multi-media WSN include high bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing and compressing techniques, and cross-layer design. Multi-media content such as a video stream requires high bandwidth in order for the content to be delivered. As a result, high data rate leads to high energy consumption. Transmission techniques that support high bandwidth and low energy consumption have to be developed. QoS provisioning is a challenging task in a multi-media WSN due to the variable delay and variable channel capacity. It is important that a certain level of QoS must be achieved for reliable content delivery. In-network processing, filtering, and compression can significantly improve network performance in terms of filtering and extracting redundant information and merging contents. Similarly, cross-layer interaction among the layers can improve the processing and the delivery process.

E. MOBILE WSNs

Mobile 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 network. A mobile WSN can start off with some initial deployment and nodes can then spread out to gather information. Information gathered by a mobile node can be communicated to another mobile node when they are within range of each other. Another key difference is data distribution. In a static WSN, data can be distributed using fixed routing or flooding while dynamic routing is used in a mobile WSN. Challenges in mobile WSN include deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, and data process. Mobile WSN applications include but are not limited to environment monitoring, target tracking, search and rescue, and real-time monitoring of hazardous material. For environmental monitoring in disaster areas, manual deployment might not be possible. With mobile sensor nodes, they can move to areas of events after deployment to provide the required coverage. In military surveillance and tracking, mobile sensor nodes can collaborate and make decisions based on the target. Mobile sensor nodes can achieve a higher degree of coverage and connectivity compared to static sensor nodes. In the presence of obstacles in the field, mobile sensor nodes can plan ahead and move appropriately to obstructed regions to increase target exposure.

Table 1: Comparison between the different types of Wireless Sensor Networks

TYPE	DEFINITION	CHALLENGES	APPLICATIONS
Terrestial WSN	A network consists of hundreds to thousands of sensor nodes deployed on land	• In-network data aggregation to improve performance across communication, energy cost, and delay • Minimizing energy cost • Reduce the amount of data communication • Finding the optimal route • Distributing energy consumption • Maintaining network connectivity • Eliminating redundancy	• Environmental Sensing and monitoring • Industrial monitoring • Surface explorations
Underground WSN	A network consists of wireless sensor nodes deployed in caves or mines or underground	• Expensive deployment maintenance, and equipment cost • Threats to device such as the environment and animal • Battery power cannot easily be replaced • Topology challenges with preplanned deployment • High levels of attenuation and signal loss in communication	• Agriculture monitoring • Landscape management • Underground structural monitoring • Underground environment monitoring of soil, water or mineral • Military border monitoring
Under Water WSN	A network consists of wireless sensor and vehicles deployed into the ocean environment	• Expensive underwater sensors • Hardware failure due to environment effects • Battery power cannot easily be replaced • Sparse deployment • Limited bandwidth • Long propagation delay, high latency and fading problems	• Pollution monitoring • Undersea Surveillance and exploration • Disaster prevention Monitoring • Seismic monitoring Equipment monitoring Underwater robotics
Multi-media WSN	A network consists of wireless sensor devices that have the ability to store, process, and retrieve multi-media data such as video, audio, and images	• In-network processing, filtering, and compressing of multi-media content • High energy consumption and bandwidth demand • Deployment based on multi-media equipment coverage • Flexible architecture to support different applications • Must integrate various wireless technologies • QoS provisioning is very difficult due to link capacity and delays • Effective cross layer design	• Enhancement to existing WSN applications such as tracking and monitoring
Mobile WSN	A network consists of mobile sensor nodes that have the ability to move	• Navigating and controlling mobile nodes • Must self-organized • Localization with mobility • Minimize energy cost • Maintaining network connectivity • In-network data processing • Data distribution • Mobility management • Minimize energy usage in locomotion Maintain adequate sensing coverage	• Environmental Monitoring • Habitat monitoring • Military surveillance • Target tracking • Underwater monitoring • Search and rescue

III. OBSTACLES OF SENSOR SECURITY

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [7].

A. VERY LIMITED RESOURCES

All security approaches require a certain amount of resources for the implementation, including data memory, code

space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

a. 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. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [8]. With such a limitation, the software built for the sensor must also be quite small. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K, and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

b. 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 sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

B. UNRELIABLE COMMUNICATION

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

a. Unreliable Transfer

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

b. Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

c. Latency

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution. Interested readers please refer to [9] on real-time communications in wireless sensor networks.

C. UNATTENDED OPERATION

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

a. Exposure to Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

b. Managed Remotely

Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamper proof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

c. No Central Management Point

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incur recently, it will make the network organization difficult, inefficient, and fragile. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

IV. SECURITY REQUIREMENTS

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own as discussed in Section 3. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following:

- A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

B. Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The advisory can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original

receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

C. Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed overtime. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

D. Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

E. Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors [10]. Several random key pre distribution schemes have been proposed in the context of symmetric encryption techniques. In the context of applying public-key cryptography techniques in sensor networks, an efficient mechanism for public-key distribution is necessary as well. In the same way that distributed sensor networks must self-organize to support multihop routing, they must also self-organize to conduct key management and building trust relation among sensors. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

F. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. In [11], the authors propose a set of secure synchronization protocols for sender-receiver (pairwise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

G. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc. A technique called verifiable multilateration (VM) is described in [12]. In multilateration, a device's position is accurately computed from a series of known reference points. In [12], authenticated ranging and distance bounding are used to ensure accurate location of a node. Because of distance bounding, an attacking node can only increase its claimed distance from a reference point. However, to ensure location consistency, an attacking node would also have to prove that its distance from another reference point is shorter [12]. Since it cannot do this, a node manipulating the localization protocol can be found. For large sensor networks, the SPINE (Secure Positioning for sensor NEtworks) algorithm is used. It is a three phase algorithm based upon verifiable multilateration [12].

H. Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

CONCLUSION

In this chapter we have described the two main aspects of wireless sensor network: Architecture & security. Within each of those categories we have also sub-categorized the major topics to provide both a general overview of the rather broad area of wireless sensor network & its security.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "*A survey on sensor networks",* IEEE Communications Magazine 40 (8) (2002) 104–112.

[2] I.F. Akyildiz, E.P. Stuntebeck, *"Wireless underground sensor networks: research challenges, Ad-Hoc Networks*" 4 (2006) 669–686.

[3] M. Li, Y. Liu, "*Underground structure monitoring with wireless sensor networks",* in Proceedings of the IPSN, Cambridge, MA, 2007.

[4] I.F. Akyildiz, D. Pompili, T. Melodia, "*Challenges for efficient communication in underwater acoustic sensor networks",* ACM Sigbed Review 1 (2) (2004) 3–8.

[5] J. Heidemann, Y. Li, A. Syed, J. Wills, W. Ye, "*Underwater sensor networking: research challenges and potential applications"*, in: Proceedings of the Technical Report ISI-TR-2005-603, USC/ Information Sciences Institute, 2005.

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

[7] D. W. Carman, P. S. Krus, and B. J. Matt. "*Constraints and approaches for distributed sensor network security".* Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[8] http://www.xbow.com/wireless home.aspx, 2006.

[9] J. A. Stankovic et al. *"Real-time communication and coordination in embedded sensor networks*", Proceedings of the IEEE , 91(7):1002–1022, July 2003.

[10] L. Eschenauer and V. D. *Gligor. "A key-management scheme for distributed sensor networks".* In Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47. ACM Press, 2002

[11] H. Chan and A. *Perrig. "Security and privacy in sensor networks".* IEEE Computer Magazine pages 103–105, 2003.

[12] S.Capkun and J.-P. Hubaux. *"Secure positioning in wireless networks".* IEEE Journal on Selected Areas in Communications, 24(2):221–232, 2006.