Survey on Security aspect of WSN

Gaurish Edake[1], Ganesh Pathak[2]

Abstract

Recently, the tremendous growth in processor, memory, and wireless technology have enabled the development of distributed networks of small, lightweight and cost effective nodes that are capable of sensing the data, computing according to need. Wireless sensor networks (WSNs) are collections of a large amount of small devices equipped with integrated sensing and wireless communication capabilities [3]. These are considered as a special case of ad hoc networks with reduced mobility. Sensor networks share some important characteristics with ad hoc networks, for example they share the need for self-organization, wireless multi-hop operation, and time-variability in topology. The sensor networks are expected to find widespread use in a variety of applications. Environmental monitoring, condition based maintenance, habitat monitoring, seismic detection, military surveillance, inventory tracking, smart spaces etc are some examples. Designing wireless networks with strict layering principle did not fulfil the expectation raised in wire line network design. Due to dynamic nature, infrastructure less architecture, limited resources, mobility of nodes and time varying unstable links and topology, the ad hoc mobile networks oppose strict layered protocol design

Keywords

Wireless sensor network, attacks, security requirement, cross-layer technique.

1. Introduction

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni- directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators[6].
The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work [7].

Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defence, and smart spaces[3].

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. The main reason is that the set of assumptions underlying previous work has changed dramatically. 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 behaviour is important and location is critical [7]. Many wireless sensor networks also utilize minimal capacity devices which places a further strain on the ability to use past solutions. The main characteristics of a WSN include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions

Gaurish M. Edake, Research Scholar, Information Technology Department, SCOE Pune, India.
Ganesh Pathak, Associate Professor, Information Technology Department, SCOE Pune, India.

- Ease of use
- Power consumption[3]

2. Security Aspects of WSN

In any environment, either physical or logical, there exists the need of maintaining someone or something safe, away from harm. This is the role of security. On any computer-related environment, security can be considered as a non-functional requirement that maintains the overall system usable and reliable, protecting the information and information systems. In fact, in wireless sensor networks, security is of paramount importance: the network must be adequately protected against malicious threats that can affect its functionality. Due to the role of sensor networks as a “sensory system”, any disturbance in a sensor network may have consequences in the real world. However, sensor networks are especially vulnerable against external and internal attacks due to their peculiar characteristics.

The devices of the network (i.e. sensor nodes) are constrained in terms of computational capabilities, memory, communication bandwidth, and battery power. As a result, it is challenging to implement and use the cryptographic algorithms and protocols required for the creation of security services.

In most cases, it is easy to physically access sensor nodes: they must be located near the physical source of the events. Since nodes are not tamper resistant due to cost constraints, any human user or machine can reprogram them or simply destroy them.

Any internal or external device can access to the information exchange because the communication channel is public. Besides, attacking the availability of the wireless channel is not a complex task.

It is a difficult task to monitor and control the actual state of the elements of the network due to the inherent distributed nature of sensor networks. Any failure in any of its elements may remain unnoticed, or the actual cause of the malfunction may not be known. Besides, a sensor network can be attacked at any point[8].

2.1 Security Threats

Due to their previously shown inherent vulnerabilities, sensor networks have to face multiple passive and active attacks that may easily hinder its functionality and nullify the benefits of using its services[3]. Passive attacks are able to retrieve data from the network, but do not influence over its behaviour. On the other hand, active attacks directly hinder the

provisioning of services. The different threats that target sensor networks will be detailed in the following paragraphs, and they can be categorized as follows:

Common Attacks. As the wireless medium is used as the main transmission channel in WSN, it is easily subject to various types of attacks, either passive (eavesdropping) or active (data injection).

Denial of Service Attacks (DoS). These attacks prevent any part of WSN from functioning correctly or in a timely manner. Such attacks can target the communication channel (e.g. jamming) or the life of the nodes themselves (e.g. power exhaustion).

Node Compromise. An embedded device is considered being compromised when an attacker, through various means, gains control or access to the node itself after it is being deployed. These attacks are usually utilized as a foundation for more powerful, damaging attacks.

Side-channel Attacks. An adversary can monitor certain physical properties of the nodes, such as electromagnetic emanation, whenever it performs a cryptographic operation. If the recorded physical values are influenced by the secret key, then the adversary can extract information about that key.

Impersonation Attacks. A malicious sensor node can create multiple fake identities (Sybil attack), and also can create duplicates with the same identity (replication attack). These types of attacks are also the initial step which enables the attacker to conduct a wide range of malicious attacks.

Protocol-specific Attacks. Some essential protocols used in WSN, such as routing, aggregation, and time synchronization, are targeted by specific attacks that aim to influence the internal services of the network. By using the so-called *common attacks class*, a malicious adversary uses a device that does not belong to the sensor network in order to access to the contents of the communication channel. The simplest instance of common attack is eavesdropping [2].

2.2 Security Requirements

As we have previously seen, sensor networks are vulnerable to external and internal attacks. The effects of those attacks in the network are not trivial, since they can render the services of the network useless. It is clear that there is the need of using security mechanisms either to prevent the attacks from influencing over the functionality of the network or to minimize the adverse effects of such attacks.[3] By using the security mechanisms, it can be possible to enforce in sensor networks the following security properties:

Confidentiality. This property tries to fulfil the following principle: A given message must not be understood by anyone other than the desired recipients. While confidentiality is an important security property, it may be not mandatory in certain scenarios where the data is public by itself (i.e. the temperature of a street) and no other information can be derived from it. Besides, certain control data exchanged by the nodes, such as security credentials and secret keys, must be hidden from unauthorized entities.

Integrity. This property states that the data produced and consumed by the sensor network must not be maliciously altered. Unlike confidentiality, integrity is, in most cases, a mandatory property.

Authentication. Informally, data authentication allows a receiver to verify that the data is really sent by the claimed sender. This security property is quite important in sensor networks. In fact, without authentication the barrier between external and internal members of the network would not exist, as any outsider could claim that it is a registered member of the network. Moreover, even existing network members could easily pose as their neighbours. This situation would encourage many problematic situations, such as adversaries forging the whole packet stream by injecting additional packets, and nodes accepting false administrative tasks (e.g. network reprogramming).

Authorization. As for this property, it states that only authorized entities (sensor nodes and base station) can be able to perform certain operations in the network (e.g. information providing, controlling the signal

Availability. The users of a sensor network must be capable of accessing its services whenever they need them. As a result, the different hardware and software elements of the network must be robust enough to be able to provide services even in the presence of malicious entities or adverse situations.

Freshness. Sensor networks are very data-centric: they exist due to the physical data they have to collect from an environment. One important property that arises from this fact is freshness: the data produced by the sensor network must be recent.

Forward and Backward Secrecy. As new sensor nodes can be deployed whenever other sensor nodes fails, there are two properties that need to be considered: forward secrecy, where a sensor should not be able to read any future messages after it leaves the network, and backward secrecy, where a joining sensor should not be able to read any previously transmitted message.

Self-Organization. One specific property related to the autonomous nature of sensor networks is self-organization: sensor nodes must be independent and flexible enough to autonomously react against problematic situations, organizing and healing them. However, as the previous statement may not be realistic, nodes should be able to at least adapt their activities to assure the continuity of the services.

Auditing. The elements of a sensor network must be able to store any significant events that occur inside the network. This property is necessary due to the autonomous nature of the nodes. As users do not operate the sensor nodes directly, but through the base station, they may not be able to know about the existence of a certain event unless the nodes store it.

Privacy and Anonymity. These security properties are very important in those scenarios where the location and identities of the base station and the nodes that generated information should be hidden or protected. Note that this property can transcend beyond the technological dimension and affect its social environment, since sensor networks could be used as a surveillance tool to collect data about the behaviour of human beings.[8]

2.3 Flaws of layered security approach and different types of attacks

WSNs interact directly with their physical environments which poses additional security challenges. Subsequently, the existing security mechanisms in the literature are inefficient and inadequate; thus, there is a need to make the WSNs immune to attacks and novel ideas[3]. There are some major drawbacks of layered security approach

Redundant security provisioning The prerequisite of maximum security services in each node may lead to depletion of system resources and may significantly reduce the longevity of the network. The unconsidered design of security provisioning may use up network resources and therefore unintentionally launch security service DoS (SSDoS) attack. Unfortunately, there may be several protocol layers within the network protocol stack which are capable of providing security services to the same attack. Consequently, when the original data go through the protocol stack starting from the highest layer, they will be processed layer-by-layer. To this end, some part of the data packets may go through the security-prerequisite operations of different layers and result in redundant security provisioning.

Inflexible security services A countermeasure scheme in some protocol layer is unlikely to warrant security provisioning all the time. For instance, link layer security scheme typically addresses confidentiality (data privacy) provisioning, authentication (source and data integrity) and data freshness, but no security issues in the physical layer. However, an insecure physical layer may practically make the entire network remain insecure. So, it is easy to figure out that cross-layer solutions can accomplish better performance.
Power inefficiency The primary concern in designing a sensor network is energy efficiency. There are various sources of power consumption in WSNs, such as idle listening, retransmissions resulting from collisions, control packet overhead, large packet size and unnecessarily high transmitting power. Correspondingly, there are various methods of reducing power consumption. Several approaches limit the transmission power aiming to increase the spatial reuse, while maintaining network connectivity.

Summary table of different kinds of attacks on WSN is drawn below:

Table 2.1. Types of attacks in layered WSN

Attack Based on	Types of attacks	
Capability of the Attacker	node compromise attacks, Passive versus active attacks, Mote-class versus laptop-class attacks	
Attacks on Information in Transit	Interruption, Interception, Modification, Fabrication, Replaying existing messages	
Subject Based	Host-based attacks, Network-based attacks	
Protocol Stack	Physical Layer	Jamming, Radio interference ,Tampering or destruction
	Data Link Layer	Continuous Channel Access ,Collision, Unfairness, Interrogation
	Network Layer	Sinkhole, Hello Flood ,Node Capture, Selective Forwarding/ Black Hole Attack, Sybil Attack, Wormhole Attacks, Spoofed, Altered, or Replayed Routing Information, Ack Spoofing, Misdirection Internet Smurf Attack, Homing
	Transport layer	Flooding, Desynchronization Attacks
	Application layer	Overwhelm attack, Path based DOS attack, Deluge (reprogram) attack

3. Cross layer security techniques for WSN

The traditional layered approach does not fit the wireless communication system design perfectly due to multiple users accessing scarce and changeable transmission media. The performances of such systems can be optimized by considering some vertical coupling between the layers. These inter- or cross layer interactions provide useful information allowing improvement of network performance.

Cross-layer optimization defines a general concept of communication between layers, considering certain smart interactions between them, and resulting in network performance improvements. It aims in coupling the functionality of network layers with the goal of boosting system-wide performance.

Traditional approach concerning OSI layered model can recognize a subset of possible cross-layer [4] interactions depicted in Fig. 3.1

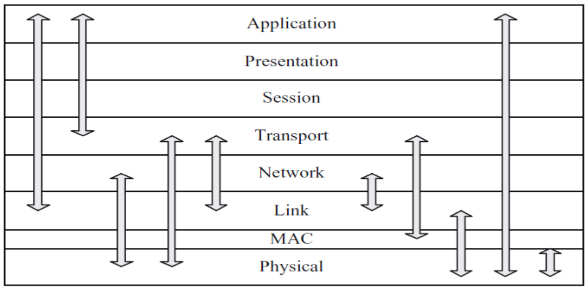

Fig. 3.1. cross-layer interactions

The key to practical cross-layer optimization is to find an appropriate abstraction of each layer and adequate coupling mechanisms. Ad hoc networking is a multilayer problem [8]. The physical layer must adapt to emerging changes in link characteristics. The multiple access control layer needs to minimize collisions and allow fair access and semi-reliable transport of data over the shared wireless links in the presence of rapid changes and hidden or exposed terminals. The network layer is responsible to determine and distribute information used to calculate paths and to maintain efficiency with changeable links and variable bandwidth.

Each layer in an ad hoc network depends on other layers, either directly or not. So, the cross-layer design that supports *adaptability* and *optimization* is needed.

Benefits of cross-layer information exchanges increase the cost of the system in sense of additional *signalling* needed to extract relevant parameters from one layer and offering it to other layer/layers. Also, more complex control plane and corresponding transmission occupied resources, increased computation complexity of the involved protocols and overhead information has to be considered. It means that whenever cross-layer approach is proposed, it must be carefully analyzed in each particular network scenario combined with carefully chosen parameters involved in optimizations.

Table 3.1. Relevant functions involved in cross-layer design

Layer	Information
Application layer	Topology control algorithm, Server location, Network Map
Transport layer	Congestion window, Timeout clock, Packet losses rate
Network layer	Routing affinity, Routing lifetime, Multiple routing
MAC/Link layer	Link bandwidth, Link quality, MAC packet delay
Physical layer	Node’s location, Movement pattern, Radio transmission range, SNR information

4. Conclusion

Wireless sensor networks are expected to be employed in the near future in a wide variety of applications, ranging from military, to industrial, to social, to domestic. Security is crucial to the success of a sensor network, because people want to guarantee a high level of service availability as well as information confidentiality and integrity in the face of potential security attacks. However, sensor networks pose unique challenges in security provisioning and layered security schemes have been shown to be inadequate and/or inefficient. The cross layer designs are expected to be the solution of choice to closely examine the trade-offs between added security, vulnerability and network performance.

References

[1] Mingbo Xiao, Xudong Wang, Guangsong Yang: “Cross-Layer Design for the Security of Wireless Sensor Networks”, in Proceedings of the 6th World Congress on Intelligent Control and Automation, Dalian, China (2006) pp 104-108.

[2] Wei Wang, Dongming Peng, Honggang Wang, Hamid Sharif: “A Cross Layer Resource Allocation Scheme for Secure Image Delivery in Wireless Sensor Networks”, in IWCMC'07, Honolulu, Hawaii, USA (2007) pp 152-157.

[3] Hosam A. Rahhali, Ihab A. Ali, Samir . Shaheen: “A Novel Trust-Based Cross-Layer Model for Wireless Sensor Networks”, in 28th NATIONAL RADIO SCIENCE CONFERENCE, National Telecommunication institute, Egypt (2011).

[4] Bin Ma: “Cross-layer trust model and algorithm of Node Selection in Wireless Sensor Networks”, in International Conference on Communication Software and Networks (2009) pp 812-815.

[5] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis: “A Security, Privacy and Trust Architecture for Wireless Sensor Networks” in 50th International Symposium ELMAR-2008, Zadar, Croatia (2008) pp 523-529.

[6] Satish V.Reve, Sonal Choudhri: “Management of Car Parking System Using Wireless Sensor Network” in International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 7, July 2012.

[7] Dr. R. Periyasamy: “Empirical evolution of DSR and AODV routing protocol in wireless sensor network” in IJST 2012, vol 2 Issue 3 june 2012.

[8] Javier Lopez,Rodrigo Roman, Cristina Alcaraz: "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks" in foundation of security analysis and design, vol 5705, in 2009.

Mr. Gaurish M. Edake is a research scholar of post-graduation in Information Technology department at Sinhgad College of Engineering, Pune. He is Computer engineer from AVCOE, Sangamner.

Mr. Ganesh R. Pathak is an Associate Professor in Information Technology department at Sinhgad College of Engineering Pune. He is one of the reputed and respectable professors in Pune University and also member of syllabus committee.