Security and Privacy Control for Wireless Sensor Networks

Sanjeev Puri
Reviewer member IACSIT, Elsevier, IEEE-ICMLC
Professor(Information Technology), SRMGPC, Lucknow, India

Abstract: To provide security and privacy to wireless sensor networks is challenging, due to the open nature of wireless communication and the limited capabilities of sensor nodes in terms of processing power, storage, bandwidth, and energy. Additionally, widespread and unrestricted deployment of WSNs makes them exposed to a number of security vulnerabilities. So we need to resolve of these problems with relevant privacy principles with legality purpose.

Index Terms: security, privacy, wireless sensor networks, power, storage, bandwidth, energy, vulnerabilities,

1. Introduction

A wireless sensor network (WSN) consists of distributed autonomous devices in sensor nets comprises hundreds or thousands of sensor nodes with sensing, computing, and communication to drill, observe, and counter to events and facts in a specified environment for a variety of applications. Each node represents a latent point of attack, making it impractical to monitor and protect each entity sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who detain and reprogram entity sensor nodes.

As WSNs are usually deployed in an environment that is vulnerable to many security attacks, it is critical to control the access to the sensor nodes, especially when there are many users in the system. Additionally, different users may have different access privileges. A centralized access control approach requires a base station to be involved whenever a user requests to get authenticate and access the information stored in the sensor nodes.

There are two types of privacy: Network Privacy-Privacy of the network itself (nodes, information) Sometimes important (battlefield), sometimes not (earthquake). Next one is Social Privacy-Privacy of the subjects under surveillance. Nodes will get smaller, cheaper. It is easy to create "surveillance" network. Get data about subjects at a "safe" distance. Need to automatic data collection, analysis and event correlation to protect privacy in networks.

The privacy and security issues posed by sensor networks stand for a rich field of research problems.
There are many general privacy problems are faced while implementing wireless sensor networks. The problems regarding mapping of data processing exist in data collection, data transmission, data usage, data storage and analysis of data. The problems related to remote data collection, tracking, unobserved data subject, data creeping, slow down of processing of data from backend, access control problem and linking of data from different resources. Therefore there is the requirement of privacy rules data binding, transparency, data storage security etc. [5]

Improving network hardware and software may address many of the issues. There are some important major issues are:

- If sensitive data is processed are there safeguards for higher protection of this type of data in place.
- Number of trust and reputation issues is a fundamental concern for operation and stability of WSNs.
- What is the purpose for which the technology will be used and data be processed?
- Can the WSN be used for other purposes than the initially intended purpose?
- Does the WSN allow for or aim at transmission of collected data to third party via an interface?
- Is a unique identifier processed?

- Are sources of data recorded?
- Is it possible to set and later change automated retention periods / data deletion?
- Does any WSN node compromise?
- Does use of the WSN affect an undefined number of individuals?
- Is data collected, processed or stored secretly / unobserved?
- Does the WSN allow for rectification of incorrect data?
- Does the WSN enable checking the accuracy of personal data with the data subject concerned?
- Are procedures in place to detect breaches of security?
- How did Node-i and Node-j manage to share a secret value
- Is it rely on an on-line central agent or implement DH key-establishment

A privacy-preserving access control in WSNs follows the following requirements. The user authentication needs to be enforced for sensor data in WSNs so that the information will not be obtained by unauthorized entities. A network user may want to hide his data access privacy from anyone else including the network owner and other network users. More specifically, anyone else should be prevented from either knowing who the sender of the query command is, or whether two query commands originate from the same unknown sender. *Node-to-node authentication* is one basic building block for enabling network nodes to prove their identity to each other. *Node revocation* can then exclude malicious nodes.[4]

The adversary may try to modify the query command constructed by a user, and a secure access control method should support the integrity protection of the query command. The adversary cannot impersonate any network user by compromising nodes. The protocol should be efficient even in a large scale WSN with many users and many nodes. To defend against replay attacks, a node should have the capability of freshness checking for any query message access restriction may be enforced for users with different access privileges. New users can easily join the network, and users can easily be revoked when they are expired. In some application scenarios, it is necessary to establish secure channels between a network user and the targeted nodes. Due to the limited energy, processing and storage resources of sensor nodes, a cryptographic technique should be efficient.

Obviously, designing a privacy-preserving access control in WSNs is a non-trivial task because wireless networks are vulnerable to attacks and sensor nodes are resource constrained. In particular, a network user hopes to protect his data access privacy from the network owner, although the network owner controls the whole network. Despite significant progress in WSNs security [7], distributed privacy-preserving access control has drawn attention only very recently. The only distributed privacy-preserving access control protocol employs the blind signature technique. Using this protocol, each anonymous user has the same access privilege. Further, we observe that it has a number of security weaknesses and efficiency.For WSNs to achieve their full potential in monitoring and control applications, manufacturers will need to focus on innovations in security and reliability to allay performance concerns. Security is the primary concern, as there is always a possibility of unauthorized access. The failures of early wireless standards such as the Wired Equivalent Privacy (WEP) were mainly due to security issues. Reliability is also a key requirement, as wireless transmission can be affected by path loss, shadow fading and ambient noise. WSNs are also susceptible to interference, which can corrupt the signal and break communication.

The future of the WSN now rests on the success of the latest authentication and encryption protocols under development, that provide greatly enhanced security as long as strict quality controls can be maintained. Emerging technologies such as Bluetooth Low Energy (BLE), ZigBee Green Power, Wi-Fi Direct and innovations from EnOcean will also enable WSNs to perform more varied applications across the medical devices, automotives, and energy-efficiency and agriculture industries, assist the success.

Wireless sensor networks are usually deployed in human unattended environments to finish some boring but security sensitive tasks, such as monitoring and target-tracking. These security-sensitive tasks wireless sensor networks are expected to engage in make them quite attractive to hostile attacks. The wireless communication, large scale and human unattended deployment make attacks in wireless sensor networks relatively easier to perform. Our goal is to analyze traffic model of sensor network and find a method for detect intrusion and abnormal sensor node behavior.

Nowadays, with more and more applications utilizing sensitive sensor information such as location context aware computing, the influence of information diffusion to privacy issues becomes more and more important. However, context-aware computing environment brings a grave threat to personal privacy protection. Whoever getting the context information is able to deduce owner's status which is not happy to share with others by owner in most cases. We introduce the concept of information diffusion to analyze privacy. We divide all systems based on user's requirements of diffusion scale into three categories: public, protected and private. We will analysis and propose the frame work and methods for privacy protection for context aware sensor network applications.

2. Privacy Problems

The main privacy problem is that much information from sensor networks could probably be collected through direct site surveillance. Another is together data at a detail level that could compromise privacy. Addressing the problem of sensor node compromise requires technological solutions. For example, cheap tamper-resistant hardware could make it.

Content Privacy means of a communication exchange that is Messages, Context. Identity Privacy deduces identities of nodes in a communication. Location Privacy infers physical position of node. Threats against content privacy and contextual privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a sensor network. This type of treats is countered by encryption and authentication. There are several ways that an adversary can trace the location of a receiver. First, an adversary can deduce the location of the receiver by analyzing the traffic rate. This is traffic-analyzing attack. Here, the basic idea is that sensor near the receiver forward a greater volume of packets than sensor further away from the receiver.

By eavesdropping the packets transmitted as various locations in a wireless sensor network, an adversary is able to compute the traffic densities at these locations, based on which it deduces the location of the direction to the receiver. To perform the traffic-rate analysis, an adversary has to stay at each location long enough such that sufficient data can be gathered for computing the traffic rate. This process takes long time as the adversary moves from location to location. Second, an adversary can reach the receiver by following the movement of packets. In packet tracing attack, an equipped adversary can reveal the location of the immediate transmitter of an overhead packet, and therefore he is able to perform hop-by-hop trace towards the original data source.

In order to protect the receiver's location privacy, a new location-privacy routing (LPR) protocol can be used to provide path diversity. This protocol can be combined with fake packet injection to minimize the information that an adversary can deduce from the overhead packets about the direction towards the receiver. Path diversity provided by LPR leads to larger routing paths, while transmitting spurious packets consumes extra energy. The stronger the protection for the receiver is required, the higher the overhead will be. Different approaches are designed to protect user's privacy in location tracking systems, which determine the positions for location-based services.

2.1 Attacks on secrecy and authentication

There are different types of attacks under this category as discussed below.

Node replication attack: In a node replication attack, an attacker attempts to add a node to an existing WSN by replication i.e. copying the node identifier of an already existing node in the network [56]. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the WSN by corrupting and forwarding the packets in wrong routes. This may also lead to network partitioning, communication of false sensor readings. In addition, if the attacker gains physical access to the entire network, it is possible for him to copy the cryptographic keys and use these keys for message communication from the replicated node. The attacker can also place the replicated node in strategic locations in the network so that he could easily manipulate a specific segment of the network, possibly causing a network partitioning.

Attacks on privacy: Since WSNs are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a WSN is particularly difficult challenge [33]. Moreover, an adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple sensor nodes. This is analogous to the panda hunter problem, where the hunter can accurately estimate the location of the panda by monitoring the traffic [57].

The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. Since the adversary need not be physically present to carry out the surveillance, the information gathering process can be done anonymously with a very low risk. In addition, remote access allows a single adversary to monitor multiple sites simultaneously [6]. Following are some of the common attacks on sensor data privacy:

Eavesdropping and passive monitoring: This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.

Traffic analysis: In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN. For example, a sudden increase in message communication between certain nodes signifies that those nodes have some specific activities and events to monitor. Deng et al have demonstrated two types of attacks that can identify the base station in a WSN without even underrating the contents of the packets being analyzed in traffic analysis [26].

Camouflage: An adversary may compromise a sensor node in a WSN and later on use that node to masquerade a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically. It may be noted from the above discussion that WSNs are vulnerable to a number of attacks at all layers of the TCP/IP protocol stack.

2.2 Defending Against Attacks on Sensor Privacy

Sensor detectors offer one possible defense against such attacks. A detector must be able not only to detect the presence of potentially hostile wireless communications within domain that may have noteworthy levels of radio interference but also to distinguish between the transmissions of authorized and unauthorized sensor networks via other devices. Such technologies might not prevent unauthorized parties from deploying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem fairly.

Regarding the attacks on privacy, there exist effective techniques to counter many of the attacks levied against a sensor. The common techniques [2][3] are.

Anonymity Mechanisms

Location information that is too specific can enable the identification of a user, or make the continued tracking of movements feasible. This is a threat to privacy. Anonymity mechanisms depersonalize the data before the data is released, which present an alternative to privacy policy-based access control.
Researchers have discussed several approaches using anonymity mechanisms, for example, Gruteser and Grunwald [26] analyze the feasibility of anonymizing location information for location-based services in an automotive

telematics environment; Beresford and Stajano [6] independently evaluate anonymity techniques for an indoor location system based on the Active Bat. Total anonymity is a difficult problem given the lack of knowledge concerning a node's location. Therefore, a tradeoff is required between anonymity and the need for public information when solving the privacy problem.

Decentralize Sensitive Data

The basic idea of this approach is to distribute the sensed location data through a spanning tree, so that no single node holds a complete view of the original data.

Secure Communication Channel

Using secure communication protocols, such as SPINS [65], the eavesdropping and active attacks can be prevented.

Change Data Traffic

De-patterning the data transmissions can protect against traffic analysis. For example, inserting some bogus data can intensively change the traffic pattern when needed.

Node Mobility

Building the sensor movable can be effective in protecting privacy, mainly the location. Location-support system is used for in-building, mobile, location dependent applications. It allows applications running on Wireless nodes to learn their physical location by using listeners that hear and analyze information from beacons spread throughout the building. Thus the location sensors can be placed on the mobile device as opposed to the building infrastructure, and the location information is not disclosed during the position determination process and the data subject can choose the parties to which the information should be transmitted.[1]

The great number of communicating nodes builds end-to-end encryption usually impractical since sensor node hardware can rarely store a large number of unique encryption keys. As an alternative, sensor network designers may opt for hop-by-hop encryption, where each sensor node stores only encryption keys shared with its instant neighbors. In this case, adversary control of a communication node gets rid of encryption's effectiveness for any communications bound for through the compromised node. This situation could be marked worse if an adversary manipulates the routing infrastructure to send many communications through a malicious node.

More robust routing protocols are one solution to this problem. Another solution is *multipath routing*, which routes parts of a message over multiple disjoint paths and reassembles them at the destination. Efficient discovery of the best disjoint paths to use for such an operation is another research challenge.

3. Conclusion

One confront is how to secure wireless communication links against eavesdropping and tampering. Overall, security is a tricky face for any system. The severe constraints and demanding environments of WSN make computer security for these systems even more challenging. Sensor networks are set to become a really omnipresent technology that will affect our daily lives in important ways. We cannot organize such a critical technology, however, without first deal with the security and privacy research challenges to ensure that it does not turn next to those whom it is meant to assistance.

References

[1] Cheng-Kang Chu, Wentao Zhu, Sherman Chow, Jianying Zhou, and Robert Deng. "Secure Mobile Subscription of Sensor-Encrypted Data". Proceedings of 2011 ACM Symposium on Information, Computer and Communications Security (AsiaCCS'11), pages 228--237, Hong Kong, China, March 2011, ACM Press.
[2] Yanjiang Yang, Jianying Zhou, Robert Deng, and Feng Bao. "Better Security Enforcement in Trusted Computing Enabled Heterogeneous Wireless Sensor Networks". Security and Communication Networks, 4(1):11--22, Wiley InterScience, January 2011.
[3] Joseph Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun-Wen Wong. "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network". International Journal of Information Security, 9(4):287--296, Springer, August 2010.
[4] Ying Qiu, Jianying Zhou, Joonsang Baek, and Javier Lopez. "Authentication and Key Establishment in Dynamic Wireless Sensor Networks". Sensors, 10(4):3718--3731, MDPI Publishing, April 2010.
[5] Joonsang Baek, Ernest Foo, Han-Chiang Tan, and Jianying Zhou. "Securing Wireless Sensor Networks - Threats and Countermeasures". Chapter 3 of "Security and Privacy in Mobile and Wireless Networking", ISBN 978-1905886-906, Troubador Publishing, February 2009.
[6] Jianying Zhou, Tanmoy Kanti Das, and Javier Lopez. "An Asynchronous Node Replication Attack in Wireless Sensor Networks". Proceedings of 2008 IFIP International Information Security Conference (SEC'08), pages 125--139, Milan, Italy, September 2008, Springer.
[7] Javier Lopez and Jianying Zhou (editors). "Wireless Sensor Network Security". ISBN 978-1-58603-813-7, Cryptology & Information Security Series, IOS Press, 2008

Prof. Sanjeev Puri: He is the Reviewer editorial member of IACSIT-IJCEE, IEEE-ICMLC and Elsevier. He is working as Professor at SRMGPC (Now SRM University), Lucknow, India. His research interests in wireless sensor networks security, grid security and protocols