Security Issues in Wireless Sensor Networks

doi:10.3991/ijoe.v6i4.1466

Daniel Sora
DRESMARA, Brasov, Romania

***Abstract*—Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. Finally, we will try to provide a general approach to planning and implementing wireless sensor networks to support the arrays of sensors needed to operate plants, conduct scientific experiments, and test components.**

***Index Terms*—Countermeasure, Threat, Security, Sensor, Wireless.**

I. INTRODUCTION

Recent technological advances have enabled the development of small-sized (a few cubic centimeters), low-cost, low-power, and multifunctional sensor devices. There are different types of sensors. Sensors are normally specialized, but sometimes a few capabilities may be available in a single sensor. They may measure distance, direction, speed, humidity, wind speed, soil makeup, temperature, chemical composition, light, vibration, motion, seismic activity, acoustic properties, strain, torque, load, pressure, and so on.

Traditionally, sensors are attached to the environment and their measurements are sent to a base station (BS) with wired communication. During the last years, a new vision of sensor nodes as autonomous devices with integrated sensing, processing, and communication capabilities has emerged. Attaching antenna for receiving signals and a transmitter enables wireless communication of sensors. Sensors also have a small processor and a small memory for coding and decoding signals, as well as for running simple communication protocols.

Recent advances in electronics and wireless network technologies have offered us access to a new era where wireless sensor networks formed by interconnected small intelligent sensing devices provide us the possibility to form smart environments. Considering the specialty of wireless sensor network, the security threats and possible countermeasures are quite different from those in Internet and Mobile Ad Hoc Networks (MANETs). On the one hand, the wireless communication, large-scale and possibly human unattended deployment make attacks in wireless sensor networks relatively easier to perform. Furthermore, all features that make sensor nodes cheap and thus sensor network application affordable, such as limited energy resource, limited bandwidth, and limited memory, also make many well-developed security mechanisms inappropriate in sensor networks. On the other hand, the user unfriendly interface makes the physical compromise of a sensor node difficult, the relatively simple communication profile makes the intrusion detection easy to perform, and also the redundant deployment makes the new type of network more fault-tolerant. Thus, we need a complete redesign of sensor network security mechanisms from technique to management.

Although a great amount of research has been devoted to the pure networking aspects, WSNs will not be successfully deployed if security, dependability, and privacy issues are not addressed adequately. These issues become more important because WSNs are usually used for very critical applications. Furthermore, WSNs are very vulnerable and thus attractive to attacks because of their limited prices and human-unattended deployment.

The primary purpose of sensor networks is to provide:

1. timely accurate data about the state of a plant so that the plant can run with maximum efficiency;
2. data to scientists as part of a complex experiment;
3. data for test and verification of components before they go into operation.

Therefore, the final decisions about which kinds of networks to use should be based on the economics of lifetime cost versus the value of the data. Thus, the deployment of sensor networks must necessarily involve business and technical considerations.

There are key functions that sensor networks should provide: safety, security, reliability, throughput, determinism, distributed intelligence, distributed controls, distributed communications, and data synchronization.

Safety and security requirements are the most important issues when selecting any information system. Obviously, the safety and security features of the selected sensor network must be commensurate with the needs of the application. For instance, some applications require components and systems that are intrinsically safe.

In recent years, the users and developers of supervisory control and data acquisition (SCADA) systems have become increasingly aware of the necessity of securing their data and control links. Securing a wireless transmission may involve both RF signal means as well as bit-encryption means. For instance, spread-spectrum signaling makes it harder for a signal to be detected or intercepted, but this does not provide a very high level of data encryption. Any system requiring secure data should also employ message encryption means. Currently, some systems employ wired-equivalent privacy (WEP) encryption. The various encryption means are constantly being upgraded as hackers develop new methods of attacking them. Also, networks must be protected from internal attacks since more than 70% of all corporate hacking is from inside the

firewall by a disgruntled employee. This involves access controls and network architecture design.

II. SECURITY THREATS IN WSNS

WSNs are becoming popular in more and more applications, because of their sensing ability in the physical world, large scale human-unattended deployment, and the most important: simple and cheap devices. A typical WSN consists of hundreds or even thousands of tiny and resource-constraint sensor nodes. These sensor nodes are distributed and deployed in uncontrollable environment for the collection of security-sensitive information. Individual sensor node relies on multihop wireless communication to deliver the sensed data to a remote base station. In a basic WSN scenario, resource constraint, wireless communication, security-sensitive data, uncontrollable environment, and even distributed deployment are all vulnerabilities. These vulnerabilities make WSNs suffer from an amazing number of security threats. WSNs can only be used in the critical applications after the potential security threats are eliminated.

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

A. Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

B. Subversion of a Node

A particular sensor might be captured, and information stored on it (such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue.

C. False Node and malicious data

An intruder might add a node to the system that feeds false data or prevents the passage of true data. Such messages also consume the scarce energy resources of the nodes. Insertion of malicious code is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary. A seized sensor network can either send false observations about the environment to a legitimate user or send observations about the monitored area to a malicious user. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. Strong authentication techniques can prevent an adversary from impersonating as a valid node in the sensor network.

D. The Sybil attack

In a Sybil attack, a single node presents multiple identities to other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets.

Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but (s)he should only be able to do so using the identities of the nodes (s)he has compromised. Using globally shared keys allows an insider to masquerade as any (possibly even nonexistent) node. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them.

E. Sinkhole attacks

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station. Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "sphere of influence", attracting all traffic destined for a base station from nodes several hops away from the compromised node.

F. Wormholes

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through it if alternate routes are significantly less attractive.

III. COUNTERMEASURES

WSN threats either violate network secrecy and authentication, such as packet spoofing, or violate network availability, such as jamming attack, or violate some other network functionalities. Generally, countermeasures to the threats in WSNs should fulfill the following security requirements:

- ***Availability***, which ensures that the desired network services are available whenever required
- ***Authentication***, which ensures that the communication from one node to another node is genuine
- ***Confidentiality***, which provides the privacy of the wireless communication channels
- ***Integrity***, which ensures that message or the entity under consideration is not altered
- ***Nonrepudiation***, which prevents malicious nodes to hide or deny their activities
- ***Freshness***, which implies that the data is recent and ensures that no adversary can replay old messages
- ***Survivability***, which ensures the acceptable level of network services even in the presence of node failures and malicious attacks
- ***Self-security***, countermeasures may introduce additional hardware and software infrastructures into the network, which must themselves be secure enough to withstand attacks

Once a plant intranet is established with convenient access points (either wireless or wired), connection locations called access points can be established for the various subnets. These subnets provide tailored networking for data-intensive portions of the plant. That is, parts of the process or plant requiring large amounts of data to be used locally may utilize specialized sensor networks that only pass a subset of the data back through the plant intranet to the company's databases. This diversification of the network provides several benefits:

4. It allows cost-effective communication nodes to be tailored to their application rather than making all nodes carry the overhead and complexity of being all things to all users.
5. It provides an additional layer of security, especially against internal "hackers."
6. It makes spectrum management more manageable since each subset of the network can utilize a different portion of the EM spectrum or at least be allocated into regions (called microcells) within which only certain modulation schemes or frequency bands are utilized.

Depending on the applications, countermeasures should also fulfill appropriate performance requirements.

Because of the resource-constraint nature of WSNs, an inevitable performance requirement for countermeasures is low-overhead. Other applicable performance requirements could be low-cost, easy deployment, real-time requirement, etc. In the real implementation, there is usually a trade-off between the security provided and the overhead introduced by the applied countermeasure.

A. Key Management

When setting up a sensor network, one of the first security requirements is to establish cryptographic keys for later secure communication. The established keys should be resilient to attacks and flexible to dynamic update. The task that supports the establishment and maintenance of key relationships between valid parties according to a security policy is called key management. Desired features of key management in sensor networks include energy awareness, localized impact of attacks, and scaling to a large number of nodes.

Recently, numerous key management schemes have been proposed for sensor networks. Many schemes, referred to as static schemes, have adopted the principle of key predistribution with the underlying assumption of a relatively static short-lived network. An emerging class of schemes, dynamic key management schemes, assumes long-lived networks requiring network rekeying for sustained security and survivability. Also, there are some special kind of key management schemes supporting in-network processing, which is an important energy-saving mechanism in many proposed WSNs.

B. Authentication

As sensor networks are mostly deployed in human-unattended environments for critical sensing measurements, the authentication of the data source as well as the data are critical concerns. Proper authentication mechanisms can provide WSNs with both sensor and user identification ability, protect the integrity and freshness of critical data, and prohibit and identify impersonating attack. Traditionally, authentication can be provided by public-key schemes as digital signature and by symmetric-key schemes as message authentication code (MAC). Besides, key-chain schemes using symmetric keys determined by asymmetric key-exchange protocols are also popular for broadcast authentication in WSNs.

C. Intrusion Detection

Security technologies, such as authentication and cryptography, can enhance the security of sensor networks. Nevertheless, these preventive mechanisms alone cannot deter all possible attacks (e.g., insider attackers possessing the key). Intrusion detection (ID), which has been successfully used in Internet, can provide a second line of defense.

ID involves the runtime gathering of data from system operation, and the subsequent analysis of the data. ID systems can be classified according to the detection techniques they use: signature-based detection, specification-based detection, and anomaly detection.

Signature-based detection needs knowledge to build attack signatures and suffers from the inability to detect unknown attacks. At current stage of sensor network development, most of known possible attacks are only imagined or copied from other mature networks like Internet. Whether these known attacks would be serious problems and whether any unknown serious attack could happen in sensor networks still remain unclear. Unlike those unclear attack signatures, people have exact knowledge about what each designed protocol functions like. If a sensor node does not act according to the protocol specification, people have high confidence to declare that node to be malicious. Such specification-based detection has an advantage of low false alarm. However, specification-based detection cannot detect malicious behaviors which do not violate protocol specifications. In that case, anomaly detection which not only detects incorrect behaviors (which violate specifications), but also detects abnormal behav-

iors (which do not violate specifications) can serve as a complement to specification-based detection strategy. In anomaly detection, profiles of normal behaviors of systems, usually established through automated training, are compared with the actual activities of systems to flag any significant deviation. Although anomaly detection has the advantage in detecting attacks other technologies cannot do, it usually suffers from a high false alarm rate. Besides the classification according to the detection techniques, ID systems can also be classified according to the place it is located. ID systems installed and run on a single node are called host-based ID system (IDS), and this kind of ID system usually use the information (e.g. system logs) acquired from the host node to detect an attack or misbehavior, and is usually only responsible for the security of the host node. ID systems which are installed on gateway nodes or separate monitors usually take network traffic as data source and are responsible for the security of a part or the whole network. This kind of ID system is called network-based IDS. Currently, most of the proposed ID systems for WSNs are network-based and use either specification-based or anomaly-based detection techniques.

D. Fault and Intrusion Tolerance

WSNs consist of a large number of tiny sensor devices that have limited power and limited sensing, computation, and wireless communication capabilities. Sensor nodes usually operate in unattended and even harsh environments, and as a result, sensor nodes are prone to failures and are vulnerable to malicious attacks. Therefore, for reliable and secure computation and communication in WSNs, fault tolerance and intrusion tolerance become two essential attributes that should be designed into WSNs. Concretely, the goal to obtain a fault and intrusion tolerant WSN can be depicted as the following problem in the design stage: minimize the total cost of a WSN, given the constraint that the expected network operation time should still be longer than the desired network lifetime even after one or several faults and intrusions happen.

Fault tolerance and intrusion tolerance are related and thus we put them together to elaborate. The common point between faults and intrusions is that they both cause errors inside the system. Therefore, the system can malfunction due to the errors caused. The difference is that faults cause errors randomly, but intrusions are usually done deliberately and will preferentially target the most important component in the system. Further, faults can exist everywhere in the system and can happen anytime, but the scopes of intrusions are subject to the abilities of attackers, In terms of available techniques, there are similarities for fault tolerance and intrusion tolerance, for example, redundancy is efficient for both fault and intrusion tolerance. However, encryption and authentication technologies are only useful for intrusion tolerance.

E. Privacy Protection

As WSN applications expand to include increasingly sensitive measurements in both military tasks and everyday life, privacy protection becomes an increasingly important concern. For example, few people may enjoy the benefits of a body area WSN, if they know that their personal data such as heart rate, blood pressure, etc. is regularly transmitted without proper privacy protection. Also, the important data sink in a battlefield surveillance WSN may be first destroyed, if its location can be traced by analyzing the volume of radio activities.

Generally, privacy in WSNs can be classified into two categories: content privacy and contextual privacy. Threats against content privacy arise due to eavesdropping and tampering. This type of threats is partially countered by encryption and authentication. However, even after strong encryption and authentication mechanisms are applied, wireless communication media still exposes contextual information about the traffic carried in the network. For example, an adversary can deduce the direction of wireless communications by eavesdropping and analyzing the patterns of network traffic. In particular, the location information about senders/receivers may be derived based on the direction of wireless communications.

F. Security Management

Security management is the process of managing, monitoring, and controlling the security related behavior of a network, and it plays an important role in network management. The primary function of security management is controlling access points to critical or sensitive data that is stored on devices attached to the network. Security management also includes the seamless integration of different security function modules, like encryption, authentication, ID, etc. Besides these, security management in WSNs should not incur too much communication, computation and storage overheads, and should be compatible with other network management functionalities.

IV. CONCLUSIONS

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

REFERENCES

[1] Y. Zhang, P. Kitsos, "Security in RFID and sensor networks," *Taylor & Francis Group, LLC*, pp. 293–322, 2009.

[2] A. K. Pathan, H.W. Lee, C. S. Hong, "Security in wireless sensor networks: issues and challenges," pp. 1044–1047 Feb. 20-22, 2006, ISBN 89-5519-129-4.

[3] S. Kaplantzis, "Security models for wireless sensor networks," March 20, 2006.

[4] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: a survey", *Chapter 17* in Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, 2006.

[5] M. Saraogi, "Security in wireless sensor networks," Department of Computer Science University of Tennessee, Knoxville.

AUTHOR

Daniel Sora is with the Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, ROMANIA (e-mail: dansora@crmra.ro).

Submitted October 2nd, 2010. Published as resubmitted by the authors October 17th, 2010.