
Hamdollah ghamgin and Mohammad Taghi Jafari

Khalkhal Branch, Islamic Azad University, Khalkhal, Iran.

Zanjan Branch, Islamic Azad University, Zanjan, Iran.

ABSTRACT

Wireless Sensor Network (WSN) is an emerging technology and day by day it is attracting the attention of researchers with its challenging characteristics and diversified application domain. The more researchers try to develop further cost and energy efficient computing devices and algorithms for WSN, the more challenging it becomes to fit the security of WSN into that constrained environment. However, security is crucial to the success of applying WSN is essential before designing WSN system. This paper studies the security problems of WSN based on its resource restricted design and deployment characteristics and the security requirements for designing a secure WSN. Also this study documents the well known attacks at the different layers of WSN and some counter measures against those attacks. Finally, this paper discusses on some defensive measures of WSN giving focus on the key management, link layer and routing security.

Key words: security, privacy, wireless, sensor, network, WSN.

Introduction

Recently, wireless sensor networks (WSN) have gained great popularity, mainly because they provide a low cost alternative to solving a great variety of real-world problems. Their low cost enables the deployment of large amounts of sensor nodes (in the order of thousands, and in the future perhaps millions), which most of the time operate under harsh environments. WSN present extreme resource limitations, mainly in available memory space and energy source. Both limitations represent great obstacles for the integration of traditional security techniques. The highly unreliable communication channels that are used in WSN and the fact that they operate unattended make the integration of security techniques even harder.

Wireless sensor networks today offer the processing capabilities of computers of a few decades ago and the industry's trend is to reduce the cost of wireless sensing nodes while maintaining the same processing power. Based on this idea, many researchers have started to face the challenge of maximizing processing capabilities and reducing energy consumption while protecting sensor networks from possible attacks.

Security Goals and Threats:

Security threats can be categorized in classes of goals. Design for security should set the following goals for the WSN under the design process: Confidentiality, Data integrity, Accountability, Availability and Controlled access (Karl and Willig, 2007).

Some common threats within these categories are eavesdropping, masquerading, authorization violation, forgery, provoking loss or modification of information, and sabotage. Each security goal will be explained in more detail and solutions are proposed when possible.

Security in Wireless Sensor Networks:

Security in wireless sensor networks will and should become a hot topic in future WSN research Security protocols should be developed and deployed in the same time as the routing and aggregation protocols, instead of adding them later on as patches to existing holes in order to create a robust platform to deploy security critical applications.

Corresponding Author: Hamdollah ghamgin. Khalkhal Branch, Islamic Azad University, Khalkhal, Iran.
Sensors are often deployed in accessible areas, which add the risk of physical attack. This is why wireless sensor networks pose unique challenges. Security protocols and techniques used in traditional wired networks cannot be applied directly. Due to the scarce resources of wireless sensor networks, sensor nodes are limited in their energy, computation, and communication capabilities. New light weight, multi layered security schemes need to be developed in order to detect and prevent the new forms of attacks these networks are subject to, while using as little as possible of the scarce resources that exist in the networks.

Confidentiality:

Information should only be revealed to authorized entities; any other entity should not be able to discover the information from eavesdropping or from reading memories. The attacker can easily get access to the information with a simple wireless receiver, unless the data is protected by cryptographically strong algorithms. WSNs pose new problems regarding this issue, because key establishment and trust setup is troublesome. Public key cryptography must usually be excluded because of the limited computational resources. Preset keys on the other hand damage the inherent flexibility that is part of the WSN architecture. If all keys must be preset, then adding and removing nodes becomes difficult. Preset keys are also dangerous to the system if even one single node becomes compromised. With WSNs compromised nodes are more common than with traditional network nodes. Because WSN nodes are numerous and physical access to them is reactively impossible to prevent. The main solution to these security issues is the use of proper security protocol for WSNs. There are several alternatives under development, but one of the more promising ones is SPINS (Security Protocols for Sensor Networks), which already functions well at least in limited cases Perrig et al., (2003).

There are very few solutions to the physical access problem. The only feasible solution is to enhance the robustness of the node casing and thrive to ensure that any attempt to get to the internals of the node would result to the self – destruction of any parts that are important to the network security. At the same time it should be remembered that this mechanism must not be so sensitive that denial of service attack could be performed just by gently knocking off one of the nodes.

Data Integrity:

The receiver of information wants to be sure that it is not modified in transit intentionally or by accident. Ideally the data should also be reliable and provide useful sensor information.

The attacker may try to feed false information to the network either directly or by manipulating the environment that the sensors use to collect measurements and other information. Falsified data can be meaningless noise, replaying of previous data or data that is purposefully targeted against the protocols that the WSN uses.

The solution to these problems is again algorithms that attempt to preserve the integrity of the data. Cryptographic algorithms are able to ensure that data can not be modified during the transit and that stale data can not be used in replay attacks.

Application level algorithms are required to ensure that single nodes can not distort the data acquisition from the whole network. Nodes with clearly false data should be detected and handled properly.

Accountability:

The entity requesting an action, or sending a packet must be uniquely identifiable.

The attacker may try to create false nodes or sinks to confuse routing protocols. If the attacker manages to impersonate a sink or a control node, he may attain total control to the WSN and use it for his own purposes.

Cryptographic algorithms seem to be the only feasible solution here as well. Nodes should be able to authenticate each other without the possibility that false nodes could perform the authentication. Properly used Cryptographic algorithms are able to ensure that digital signatures can not be forged and that the sender of the message is who he says he is.

Availability:

Legitimate entities should be able to access the resources and illegitimate entities should not be able to render the resources inaccessible.
The most common attack against the availability of the WSN is called denial of service. This can be performed in numerous ways, starting from unsophisticated attacks like destroying certain percentage of the WSN nodes (i.e. sabotage). To the highly sophisticated attacks against the protocols that the WSN uses.

Radio channel jamming is one of the most likely ways to accomplish denial of service attack. It can be assumed that the attacker has always larger power budget than the any of the WSN nodes and is also able to continue jamming indefinitely.

Destroying certain percentage of the nodes can have the same effect as jamming, since routing protocols typically require certain density of nodes across the WSN.

The attacker can also exploit the radio channel protocols knowledge to target, for example, power saving features of the protocols. It is often possible to stave the node very quickly by making it to wake up too often by exploiting some certain feature of the protocols.

If attacker has access to the data transmitted. He may be able to modify it. The result may be routing protocols confusion or starvation of the whole network if enough of the nodes can be tricked to waste all their resources too soon.

Availability is such a multi faceted area of security that it requires multiple tools, and even then perfect security is not attainable.

Radio channel access should be made as robust as possible. The most promising technology in this regard is spread – spectrum communications, like ultra wide band (UWB), which use so large frequency band that attacker must use enormous amount of power to jam the whole frequency band. UWB also provides further layer of security because it is very difficult to detect from background noise unless the attacker knows what to look for Oppermann et al., (2004).

WSN nodes should also be able to detect radio channel jamming or attempts to starve the node. Since the attacker is assumed to have large power budget, the node must be able to figure out if any of the messages can be passed on, and if not, and then wait until the attack is over. If some messages can still be passed on by using more power, then the node might have to balance the power budget by sending message can still be passed on by using more power, then the node might have to balance the power budget by sending message less often or use alternate route to the sink or other nodes.

Cryptographic

Against attempts

Generation of false service requests. These requirements are directly connected to the security goals of data confidentiality and integrity.

**Controlled Access:**

A service or information access should only be granted to authorize entities.

The attacker may try to gain access to the WSN and, for example, command it to shut down or continue to use it for his own purposes. Access can be gained physically or by manipulating WSN nodes and traffic between them.

Physical access should be restricted as for as possible. It is unlikely that all the nodes could be protected this way, but sinks and control nodes should be protected against physical access if at all possible.

Properly executed WSN security protocols are able to precede the network against data manipulation and compromised single nodes. However, application level security is paramount to achieve the goal of controlled access to the network. Low level Cryptographic protocols are powerless if the controlling application is wide open to unauthorized users.

**Cryptographic Considerations:**

Cryptographic algorithms are such a central theme in WSN security that it deserves special attention. There are several algorithms that are proven to be secure and reliable, but most of them are note optimized for limited computing resources. All these algorithms can be divided into two categories based on the way keys for encryption and decryption are handled.

The most complicated issue with secure protocols is key exchange; a lot of effort has been put into this detail, because of special circumstances that WSNs are in.

**Symmetric and Asymmetric Algorithms:**

There are two basic methods that modern encryption algorithms use. Symmetric encryption uses the same key for encryption. The key size is relatively small, typically 128 – 256 bits. Symmetric encryption extremely efficient, easy on computational resources and can be used to quickly encrypt or decrypt large masses of data.

The problem with symmetric encryption lies in key exchange. Since the same key is used to encryption and decryption, it must be always transmitted over secure channel. This limitation is difficult to overcome in WSNs unless all the nodes have predefined keys, which in turn briefly touched upon in previous chapter.

Asymmetric encryption is based on different approach, where one key is used to encrypt data and another key to decrypt it. These keys can not be derived from each other, and typically one key is kept private whereas the other can be released into public. This method of working is commonly called Public–key Cryptographic. This technology enables secure exchange of data, encryption keys, and digital signatures and is the basis for such internet standards as Transport Layer security.

The mathematics behind public – key Cryptographic relies on the difficulty of dividing very large numbers into is prime number components. The handled numbers are so large that encryption keys can be 2048 bits or longer. Encryption with such large keys becomes computationally intensive even with the fastest systems available and is there fore commonly only used for symmetric key exchange MS, A. (2002).

Key Exchange:

Key exchange and setting up trust is one of the main challenges faced by secure WSN protocols. The reason for this is that limited computational capacity currently excludes protocols based on symmetric encryption. This fact may not change in near future, because any gains in capacity is rather used to build cheaper and more numerous WSN nodes.

Another problem is that WSN systems are usually built on ad hoc basis without any predetermined topological setup. The number of nodes and their relation is rarely known before deployment, and even if they were, the dynamic nature of the WSN demands that nodes may fail or new nodes appear at any time. This means that predetermined and stored keys for all the nodes in the WSN would likely take too much memory and would not allow any changes to the WSN later on.

Additionally, any node that is compromised by an adversary, would instantly compromise by an adversary, would instantly compromise the entire network, which is unacceptable from the security point of view. Last of the currently recognized problems is how to exchange keys in a way that scales to large WSN sizes.

It seems that many protocols would perform well in laboratory with small number of interconnected WSN nodes. In these protocols key distribution overhead may increase in square or cubic manner, which means that even moderately sized WSNs, would halt at once by the sheer amount of key exchange traffic. (Liu and Ning, 2006)

Spins:

Spins stands for Security Protocols for Sensor Networks and is a suite of security building blocks proposed by perig et al. It is optimized for resource constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and Utesla.

SNEP provides data confidentiality, two–party data authentication, and data freshness. UTESLA provides authenticated broadcast for severely resource–constrained environments. All Cryptographic primitives (i.e. encryption, message authentication code (MAC), hash, random number generator) are constructed out of a single block cipher for code reduces overhead and memory footprint of the security solution.

In a broadcast medium such as a WSN, data authentication through a symmetric mechanism cannot be applied as all the receivers know they key. UTESLA constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one–way function key chains. (Saraogi, 2001; Maronna, 2006; Brutch, 2003).

Data Aggregation:

What Is Data Aggregation:

Data aggregation is a process in which information is gathered and expressed in a summary form. Data aggregation is mostly used when we want to obtain information about particular groups based on some kind of variable. As an example we might be interested in knowing how our self. In this case the information is income and the variables are location and job situation. If we have a data base with information about individual income and personal information, like work place and living location, we could aggregation the data and produce a mean value, or perhaps a max value, of the income of people in the same situation as our self.
Data Aggregation in Wireless Sensor Network:

Data aggregation is a fundamental part of energy saving in wireless sensor networks. As a result of energy resources being scarce and communication between nodes being the most power hungry operations, reducing the amount of communication is essential to prolong the network lifetime. Data aggregation helps to reduce the communication in cluster based network topologies by allowing only the cluster heads or appointed aggregation nodes to forward data to the receiver (i.e the base station or a sink). The data aggregator node receives sensor data results from sensor nodes and does some computations on the data to produce a collective view of the observed physical phenomenon. This computation could be simply finding a mean value of the observations in that nodes area. This aggregation result is then forwarded towards the destination as a single observation instead of having every single sensor node convey their result to the destination, and by doing so using considerably more energy resources.

Results and discussion

Most security threats faced by WSNs do have solutions. Often the solution comes from Cryptographic algorithms but require great care because of limited computing resources. The most server threat that does not have an easy solution, in large areas. Physical access is a serious threat also to the Cryptographic algorithms, because keys can easily become compromised. Power constraints are another problem with very few solutions, because the adversary can be expected to have more energy resources available than any of the WSN nodes.

Authenticity and integrity:

Only providing data confidentiality is not enough to ensure the data security in WSN. As an adversary can change messages on communication or inject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. Whereas, data authentication ensures the receiver that the data hands not been modified during the transmission.

Conclusions:

The modern internet era has shown that network security is a continuing challenge. The cost of security breach can become huge in monetary terms as well as in human lives. WSN will have all this of bear and uniquely also the threat where unauthorized physical access to the network nodes can not be realistically prevented. Further research is needed in almost all of the security goal categories to alleviate.

References