Survey on Security Challenges as Related to Wireless Sensor Networks

Shawn Loveric, Michael Sieffert
University of Binghamton
{loverics, sieffert}@ainfosec.com

Abstract
Wireless sensor networks (WSN) are confronted with many security challenges. Their wireless nature and ever increasing range of usage present many unique challenges to designers of security mechanisms and protocols for WSN’s. While the security practices employed in more traditional wired networks have been scrutinized and enhanced for years [2], the relative youth of security in the wireless world is apparent as a large number of security concerns are constantly being raised, exploited, investigated, and mitigated whenever possible. We present a survey of some of the most critical aspects of security that are being addressed along with common attack techniques and defense methods.

Introduction
Wireless sensor networks are still a relatively new addition to the computing and sensing arenas. They have been used in many different scenarios to collect and sample a wide range of data. Their usefulness has been steadily increasing for a number of years and their potential uses in the future are growing astronomically as research and experimentation advance the state of the art.

As progress is made, however, certain areas are brought to light that reveal shortcomings and oversights occurring in the development of the technology powering WSN’s. The area that this paper focuses on is that of security and the mammoth amount of threats and vulnerabilities inherent in the deployment and utilization of these networks.

Perhaps the most important consideration for security in sensor networks is the tradeoff of resources vs. security. Stereotypically in network security the main consideration is usability vs. risk. There is a direct relation between accepted risk and the usability of a given system. While this tradeoff is still important in the field of sensor networks, the tradeoff of efficiency vs. security has a more profound effect. To put this notion into perspective one should consider the usefulness of the latest and greatest encryption scheme if it is resource intensive and potentially reduces the battery life of a sensor by 50 to 75 percent.

With this in mind our focus in this paper involves a discussion of the great number of attacks available to a malicious entity on or around sensor networks, ways to mitigate the risk associated with those attacks when possible, and goals for the design and implementation of future security mechanisms put in place.

Security has many facets and is of the utmost importance to the acceptance and deployment of wireless sensor networks in the future. There is great anticipation for the many uses of WSN’s in the future, including a large number of military applications, structural integrity applications, and numerous applications in locations that are inhospitable to humans. Before they will be utilized in any of these scenarios, however, the people relying on the successful collection and retrieval of data from the networks must be provided with a sense of trust in the technology. They will require that the security mechanisms and protocols used by the network provide an adequate level of protection against not only physical threats to the devices like destruction and interference, but also against the determined attacker seeking to minimize the effectiveness of the network itself and the information extracted from it.

Attackers
Research into security of any computing platform or computer network must begin with a clear understanding of the threat posed by an attacker. It is important to be aware of the possible motives that an attacker has in seeking to disrupt the security of a network, as well as his limitations.
The motives of an attacker targeting a WSN do not differ greatly from an attacker targeting a more traditional computer network and lead to similar goals. These usually fall under the category of either denying or disrupting an existing service and are discussed below.

One primary goal of an attacker is that of data corruption. An attacker of a WSN is aware that the network was deployed to collect information deemed important to some monitoring person or organization. For any deployed network, it is likely that higher level decisions are being made based on information collected and returned to the viewer. Therefore the ability to modify data on transit from sensor nodes, where data was collected, on route to the base station becomes valuable. If the attacker wishes to mislead the decision makers viewing collected information, it is possible that even minor perturbations of the data can cause significant results. On the other hand, if the attacker is knowledgeable about the data being collected, data can be mangled in such a way as to totally disguise the true nature of the environment that the sensor nodes are monitoring.

Another goal of an attacker is simply to stop the proper functioning of the network. This category of attack includes denial of service attacks, one of which is resource consumption. This attack simply strives to stop proper functioning of the network by causing energy to be used in an extremely inefficient manner. The Achilles Heal of sensor nodes is the energy supply available to them. Energy exhaustion leads immediately leads to permanent death for current sensor nodes.

A much less obtrusive attack on the security of a sensor network is eavesdropping [4]. An attacker, once within radio range of a WSN, can passively receive all radio communication taking place around it. Without proper protection of data, the eavesdropper obtains valuable information. In certain instances of network deployments, this type of attack is just as damaging as if the network is brought down altogether.

Sensor networks are deployed in a plethora of environment types. For many deployments, the environment is well studied beforehand and well understood by the persons responsible for its placement. In these situations, much can be inferred regarding the possible threats to the network. In others situations, less is known regarding the eventual surroundings of the sensor nodes or the possible threats. This situational knowledge of the network’s environment is crucial to understanding the security mechanisms that need to be put in place, as it rules out certain attacks that need to be countered.

For instance, [4] points out that there is a clear and important distinction between an attacker that is subject to the same constraints as each node on the network and the attacker that is able to place a foreign, more powerful, device in the network’s proximity. In the first case, the attacker is either on a node original to the network or on a similar node that the attacker was able to inject into the same location as the deployed WSN. In the latter case, the attacker is generally considered free of any constraints attributed to network nodes. For example, he might possess a laptop computer complete with a higher power and more sophisticated antenna. One could even fathom the attacker possessing a large array of specialized radio communication devices that communicate out-of-band compared to the WSN with multiple desktop class computers to aid in any computational or power requirements. Obviously, this type of attack allows the attacker the most flexibility and power and lead to a more challenging design phase for a security architecture.

Listing every reason for attacks on a WSN or every option available to the attacker would be impossible. It is apparent, however, that much consideration must be given to the notion of a determined attacker as security is developed for these networks.

Routing
Routing refers to the process of transmitting a piece of information, generally a packet for computer networks, from a source to a destination. This transmission will in many cases involve multiple intermediary stops while the information is en route. In wireless sensor networks, there are a few different methods of determining how routing decisions are made. Each one has its advantages, but each also is susceptible to a unique set of attacks. The main routing methodologies are discussed below, and the following section will discuss attacks against them.
First, there is the notion of geographic routing [1]. This type of routing depends on the nodes in the network possessing knowledge regarding the physical locations of other nodes in the network. Knowledge of the network layout allows a node to determine which of its neighbors is closest to the destination and route packets through it. The assumption is that the packets’ traversal along the shortest distance from source to destination will yield short transmission times.

Next, there is the method of choosing the path from source to destination consisting of the smallest number of hops, or intermediary nodes along the transmission route. At each hop there is likely to be a non-negligible delay due to things like contention for the radio bandwidth, congestion, network aggregation and processing. These delays can add up to significant amounts of time that a packet sits idle as it makes its way to the destination on the network and is the reason why the fewest number of hops might actually be the fastest way to get from place to place on the network.

Finally, routing decisions can also be made with regard to the quality of the path as determined by either link quality or the reliability rating achieved. A node can choose to send a packet to its neighbor based on perceived quality of the link. In some cases, reliability of transmission is even more important than the time it takes to reach its destination. Alternatively, the reliability of a path can be determined over a period of time as a node transmits multiple pieces of data. In this manner, a node can choose to send it down the link that it sees as having the largest chance of a successful transmission.

**Attacks on Routing**

This section details a few of the most common attacks against routing protocols on wireless sensor networks. High level descriptions of each are presented, and the attack methods used to achieve these attacks are outlined in the next section.

One type of attack against the routing of information on sensor networks is known as a Black Hole attack [4]. This type of attack can be made against just about any form of routing methodology and against all existing routing protocols. In it, the attacker aims to position himself on the path of data traversing the network. Once he is on the path, he simply does not transmit any data that would normally be forwarded in the proper handling of the protocol. In doing so, all information passing through the attacking node is silently dropped and never reaches its destination. In protocols that do not have redundancy built into the data transmission, along disjoint routes for instance, the data has no chance of being collected by the base station or analyzed. One slight modification to this attacker is often referred to as a selective forwarding attack [4]. Instead of data simply being dropped with no regard to its value, the attacker selects certain criteria that allows for some packets to be forwarded. Using this technique the adversary increases the covertness of the attack, or ability to remain undetected. He also can taint the results of the data collected by only submitting data that meets certain constraints.

There are a number of ways, depending on the protocol being used, that an attacker can mount an attack like a black hole attack. One such method is referred to as a rushing attack [5]. Rushing attacks exploit the nature of on-demand routing protocols that rely on route request transactions. Route requests occur prior to data being sent to a base station in order to determine the route that data must take in order to reach the base station. In this type of attack, the attacking node simply forwards received route requests to his neighbors before they hear the route request from other nodes. The attacker is ‘rushing’ the request out and disregarding any protocol rules that specify timeout or delay values prior to forwarding. This sort of attack makes sure that he will be on the route between the source and destination.

Another type of attack is called a sinkhole attack [4] and is closely related to the Black Hole attack. To perform the sinkhole attack the attacker attempts to position himself on the path of all network traffic, or as many paths of data flow as possible. In this manner, all network traffic is drawn towards the “sink hole” node of the attacker. This provides the attacker much more opportunity to disrupt the activity and effectiveness of the sensor network. Any data flowing through the attacking node is subject to being dropped or tampered with. Figure 1 gives an illustration of network flows during this type of attack.
A Sybil attack [4] usually targets geographical routing protocols and occurs when an attacker claims to be in many places at once. In non-geographical routing protocols, the attacker claims to have many different identities. In doing so, he greatly increases his chances of negatively affecting network activity. If every node in a network believes the attacking node to be its neighbor, for instance, then there is a good chance that the attacker can position himself on the path of data flow to enable Black Hole, Sinkhole, and Selective Forwarding Attacks.

Each of the above attacks can be performed by a node class attacker, and do not require any enhanced capabilities by an attacker. Different attacks become an issue when the attacker is assumed to be without the constraints of the regular network nodes. This type of attacker is referred to as a laptop class attacker.

One of the most dangerous attacks against a wireless sensor network is referred to as a Wormhole attack [4]. Wormhole attacks are performed by a laptop class attacker and involve an adversary with more resources at his disposal than a typical attacker on a regular network node. This type of attack occurs when two attacking nodes collaborate to deceive the rest of the network. They do so by possessing an out of band, and often times much higher bandwidth, communication channel between themselves. By doing this, the attackers effectively remove the distance between them by enabling communication to occur in an extremely fast and efficient manner. This communication will always beat the transmission of packets traversing the same distance through the legitimate communication channel.

Once an attacker has the Wormhole attack established, it becomes trivial to fake an extremely efficient and short path to the base station to the rest of the network. Therefore, this attack is an enabler for other types of attacks including Black Hole attacks, Sinkhole attacks, and selective forwarding attacks.

Denial of Service Attacks
An attacker may simply wish to stop the network from functioning or disrupt its service. Many of the previously mentioned attacks could be considered some form of denial of service, especially the Black Hole attack which just drops all traffic whenever given the chance. Other methods of denial of service are extremely unsophisticated, however, yet are also able to achieve a similar goal.

One method of attacking a sensor network deals with the weak point of all such networks up to this point. Specifically, energy consumption is one of the scarcest resources available to a network and can be the first thing that can cause it to stop functioning. An attack as simple as a malicious node constantly attempting to communicate with its neighboring nodes and not allowing the sleep cycles that are crucial to the longevity of a WSN can bring networks to a halt. Often times the entire energy supply of sensor node can be exhausted in as little as two weeks if it is under constant bombardment, whereas a node not under the same attack can last up to a few years in a similar environment.

If an attack consists of multiple malicious nodes, they can collaborate in order to monopolize the communication medium. Doing so could prevent the correctly functioning nodes on the network from ever being able to communicate due to its constant use.

Denial of service attacks although usually simple are the most difficult attacks to defend against. Unfortunately, they are often dismissed from consideration as secure communication and routing mechanisms are developed.

Data Aggregation Attacks
Data aggregation is an important building block for sensor networks that enables the collection of data and results while addressing power conservation. While data aggregation techniques are useful in extending battery life of sensor networks most fail to meet the needs of security such as data integrity, especially when a single node is compromised.

Some aggregation techniques are inherently insecure. Wagner shows that functions average,
sum, minimum and maximum are insecure while functions like count can be secured [7]. At first glance these attacks may not seem feasible, but in fact they are very trivial. A simple example is that of a building heating system that is controlled by a sensor network. Consider a configuration in which the sensor network computes the average temperature of the environment. A single user can impact the temperature of the controlled space by introducing an extreme temperature thereby directly manipulating a sensor. If the value is extreme enough once averaged into the resulting value the sensors could trigger the heating or cooling systems to activate.

The trivial nature of aggregation attacks can and will have an impact sensor networks. In fact several existing systems are vulnerable to these attacks including TinyDB, Cougar and SensorWare. Not only does TinyDB utilize the above mentioned insecure aggregation functions, but it also uses those functions as building blocks to implement these functions in a temporal manner.

**Attack Methods**

An attacker has many methods of attack. If he is in the proximity of the sensor network, then physical compromises cannot be ruled out. An attacker, with a node in hand, could compromise its physical security and place it back onto the network. The authors have found no paper dealing with defense against this type of attack.

As mentioned in the discussion of the Wormhole attack, an attacker can outfit his attacking node with a specialized antenna that can be used with other attacking nodes for a collaborative attack on a network. Another option is to simply add a more powerful antenna to a node so that it can receive and transmit to nodes further away than its neighboring nodes, giving it an advantage in most routing protocols.

**Defenses**

Up to this point our focus has been the attacks used to exploit the vulnerabilities associated with sensor networks. The following sections detail a subset of defenses mechanisms that are currently being researched within the field of sensor networks.

**Security Infrastructures and Protocols as a basis for Secure Routing**

Perhaps one of the most complete approaches to securing WSN was purposed in the project Security Protocols for Sensor Networks (SPINS) [8]. The SPINS project provides two main contributions – the Secure Network Encryption Protocol (SNEP) and the micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol (µTESLA). These contributions were applied to the basic communication patterns, observed by the authors of the SPINS paper, which include node to base station, base station to node and base station broadcast messages.

The main goal of SNEP is to provide data confidentiality, two-party data authentication and a notion that Perrig, Szewczyk, Wen, Culler, and Tygar refer to as data freshness. Data freshness is a concept in which the data is recent data that no attacker has replayed old data or that a node was suppressed from sending data in a timely manner. SNEP takes into consideration the limited computational and memory resources available to each node and as such takes a simplistic approach to cryptographic algorithms and primitives. Encryption, message authentication codes, hash and random number generation algorithms utilized by SNEP are based off a single block cipher for code reuse. It would be interesting to see further details and an implementation of this cryptographic system to investigate the inherent strength and weaknesses of the system. For example SNEP uses a MAC function for pseudo random number generation, to address the problem of entropy; it would be interesting to see a further analysis of this function.

SNEP does have some useful properties. The most interesting of which are symmetric security, replay protection and low communication overhead. Symmetric security ensures that the same message is encrypted differently each time. By utilizing a counter in the MAC SNEP provides a mechanism for eliminating replay attacks. This same counter is stored locally to each node to reduce the communication overhead.

µTESLA primarily addresses the need for an authenticated broadcast mechanism in WSN. The authors of the SPINS paper addressed some of the fundamental issues with the standard
TESLA as applied to WSN mainly the focusing on communication overhead and expensiveness of certain asymmetric encryption algorithms. Thereby μTESLA was designed to use the symmetric mechanisms provided by SNEP to authenticate the first packet in a broadcast message. μTESLA also incorporates the use of a time-released key chain to eliminate the need to store a full chain on each node, which is impractical and in most cases impossible due to the limited program store available. It should be noted that the bootstrapping mechanism for the symmetric encryption scheme used by μTESLA is a potential point of attack. In this system each node needs to know one authentic key of the one-way key chain, which implies that great care should be taken in the distribution of that key.

By addressing the security issues associated with the primary communication patterns in WSN the SPINS project appears to provide an efficient, secure infrastructure on which WSN can communicate. This secure infrastructure could be used as a basis for secure routing.

DoS Defenses
As mentioned previously in this paper a variety of attacks can be classified as denial of service (DoS) attacks. While attacks of this class are usually trivial to implement they can and are difficult to defend against. While DoS attacks can be a nuisance in wired networks they can totally decimate the functionality of a WSN.

![Figure 2 - Sensor network layers, DoS attacks and defenses [10].](image)

Several other DoS attacks are outlined in [10] and some defensive methods were also discussed. Figure 2 presents a list DoS attacks as associated with the given network layer and an accompanying countermeasure.

While Wood and Stankovic discussion general DoS attacks and countermeasures, Deng, Han and Mishra focus on a particular type of DoS attack – the Path-base Denial of Service (PDoS). A PDoS is an attack in which the attacker overwhelsms the nodes in a WSN a long distance away by flooding a multihop end-to-end communication path with either replayed packets or random injected packets [9].

Deng, Han and Mishra propose a solution for PDoS based utilizing one-way hash chains to protect end-to-end communication paths. In their scheme a one-way hash chain is a sequence of numbers such that it is trivial to compute $y = F(x)$, but computationally infeasible to compute $x = F^{-1}(y)$.

Each given node utilizes the hash chain to validate the data that is transmitted from one node to the next. When a given node receives the packet it will systematically cycle through the chain to validate that data is from a trusted source. If the data cannot be validated the packet is dropped. Figure 3 presents in this process [9].

Deng, Han and Mishra also describe mechanisms for bootstrapping an initial one-way hash chain number to the nodes in a WSN. They suggest that the initial bootstrap can be accomplished through the base station applying a public key scheme or a secure broadcast mechanism such as μTESLA. It should be noted that the bootstrapping mechanism is once again a point of weakness. If the initial one-way hash value is not distributed in a secure manner the system can and will be exploited.

![Figure 3 - Defending against PDoS attacks with a one-way hash chain [9].](image)
Secure and Resilient Aggregation
As discussed in the Data Aggregation Attacks section many of the primary aggregation functions are inherently insecure. Wagner proposes a theoretical solution to these insecure functions called resilient aggregation [7]. The notion of resilient aggregation refers to aggregation methods that can withstand perturbations in a small subset of nodes. Wagner then goes on to define several techniques for implementing resilient aggregation in a WSN.

Instead of starting anew, Wagner utilizes estimation theory to provide a basis for resilient aggregation. With this basis he shows that estimators can be created for location, average, sum, minimum, maximum, count, and median functions. Some of the tools that he utilizes to achieve the desired affect are truncation and trimming. In truncation upper and low bounds are placed on given data sets. These bounds are defined by what would be an acceptable range for a given sensor. For example if the temperature for a known location normally oscillates between -40F and 100F values outside this range could be marked as being unacceptable or at least tagged as non-normal data values. By trimming, a given percent is ignored from the highest and lowest values in the range. This percentage will must likely be dependent upon several factors including known conditions and type of data set.

Another group of researchers, Hu and Evans, take a different approach to secure aggregation. Their approach is based on two key ideas delayed aggregation and delayed authentication.

In a delayed aggregation system messages are not aggregated at the immediate next hop, instead messages are forwarded unmolested to the second hop at which point the data is aggregated. Hu and Evans observed that delayed aggregation increases the expense of transmission, but enables integrity guarantees where consecutive nodes have not been compromised. This scheme also allows for the use of symmetric keys that are distributed to node that needs to authenticate after a given time delay.

Hu and Evans’ approach deals more with securing the communication paths than the aggregation functions themselves. Both approaches are valid and perhaps both could be leveraged to create more secure and resilient means for providing data aggregation.

Discussion
It would seem that security for wireless sensor networks is still in the infant phase as it compares to the state of security in the wired networking world. It has become apparent that, as new technologies are developed, security is often times viewed as a bolt-on solution that can be overlooked during design and development and then added on later. This has been shown to be a poor paradigm for security architecture in the past, and those developing protocols for state of the art sensor networks must be keenly aware of the threats that their networks will face. In-depth scrutiny of design decisions at an early phase is almost always worth the effort and pays off in the security challenges that will inevitably face every piece of technology deployed.

Security architects have their work cut out for them in the future and likely will not benefit from increases in computational power, communication bandwidth and reliability, or energy available to the nodes in sensor networks. Rather, it is very likely that the increase in state of the art (e.g. Moore’s law) will be used to decrease the cost of components that comprise sensor nodes as well as their size, rather than increasing the power of any resource available to the sensor nodes themselves [3].

Conclusion
This paper has provided a survey of security issues as related to wireless sensor networks. We have highlighted that security in WSN is more a complex problem than in traditional wired computer networks or even wireless computers networks due to the limited computational and power resources available to sensor nodes.

Common attacks such as DoS, BlackHoles, Wormholes and Sybil were discussed along with some trivial, yet perhaps more subtle, issues such as data aggregation insecurities. Current defense methodologies were also presented and critiqued where appropriate. As a research field WSN security is still budding and new techniques for securing wireless communications under low power and computational resources will continue to be of interest as WSN as a whole continues to grow. As the applications WSN extend into more military and other sensitive markets such
as health care and financial sectors WSN security measures will come under even more scrutiny.

References


