Wireless Sensor Networks

A survey of modern approaches in security

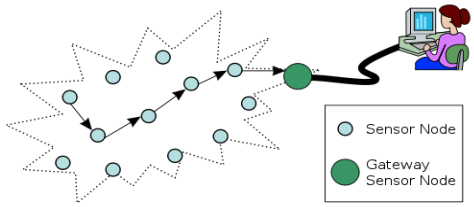
Trenton D Scott
Department of Computer Science
Missouri State University
Springfield, Mo USA

Abstract: As wireless sensor networks grow in popularity and practicality, so does the security risk of such networks. Wireless sensor networks, or WSN's, have become useful in many fields like battlefield surveillance, patient monitoring, and environmental research. By nature, these networks pose a security problem because they are low on resources, easy to implement, and highly expandable. With such important tasks at hand, security in this type of network is very important. A breach of security could mean loss of lives, blown missions, or failure to notify civilians of a natural disaster that is about to happen. This survey is intended to try and fill some of those holes with modern research on wireless sensor network and how to implement effective security.

Keywords – Wireless Sensor Networks, Mesh Networks, WSN, Network Security, Automation, Portable Ad-Hoc, Portable Networks

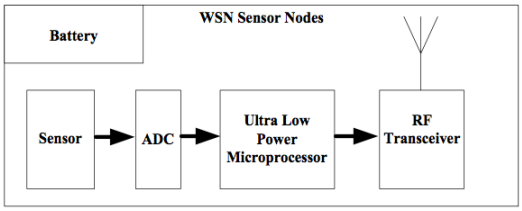
I. INTRODUCTION

To start off with, I would like to explain what I wireless sensor network is. You cannot understand if an implementation of security is effective if you do not understand why is should be implemented or the things that it is protecting. A wireless sensor network is a combination of two (sometimes three) main parts: The main unit and the child nodes (motes). The third part that is optional is the implementation of cloud computing into the model. The physical components connect via radio signals to form a mesh like network.



https://upload.wikimedia.org/wikipedia/commons/thumb/2/21/WSN.svg/500px-WSN.svg.png

The main unit is responsible for receiving the data from the child units and sending it to the cloud (or server that is set up to process and monitor the information. The main unit has the most processing and battery power because its tasks tend to take a bit more work. The main unit also should have more power in general because it can require a better transmitter to send data at longer distances.



http://www-users.york.ac.uk/~yw679/styled-6/styled-3/styled/files/snip20120802_2.png

Next is the child node. The child node or mote is responsible for the detection. You can think of it as the sensor that collects data even though there is a lot more to this small device than that. The node consists of a radio transmitter (generally omni-directional), a main board that processes the data, the battery, and finally the actual

sensor. Due to the constraints of portability and cost verses processing power, the nodes tend to be comprised of the least expensive parts to complete the job. The reasoning for going with less costly parts is because a WSN can theoretically have an unlimited number of nodes. Likewise, even if you keep the cost of an individual node low, the overall cost of the sensor network could be very expensive.

The wireless sensors can range from just a few to in the thousands and are spread across terrain, or just about any other environment that you would like. If you can imagine a net that is about how they are spread out, with the cross sections of the net being the sensors with no connecting wire. When one of the sensors are triggered, they send information back to the main unit using other nodes as a link to it.

Sensor nodes already account for things like data loss and node failure, so that will not be covered in this paper. I will go over some security problems and solutions that should be taken if you want your network to be secure.

II. SECURITY CONCERNS

The most common type of attack on WSN's is the addition of a malicious node to the network. When this node is inserted into the network it joins it as if it is not a fake node at all. This is a problem in wireless sensor networks because they are made to be so scalable that by nature, they are supposed to accept new nodes without a problem. In battlefield surveillance, if a foreign node is introduced to the network then the enemy could have full access to spoofing different values in your network and providing you with invalid information. With access of this mote, they could also stop signals when being passed through it, rendering your WSN ineffective.

Another common problem with a WSN is that the nodes have very little processing power. This is because these devices are powered by a battery. The more processing power that a device has, the more battery it takes. The problem lies within this fact, the sensor nodes can be easily overloaded. In a distributed attack where signals send requests to each node over and over the network will be useless. This could also be known as a flooding attack.

Tying into the last problem, sensors can also fail due to general causes, or be destroyed. When a sensor is destroyed, a hole in the network is introduced. If a node attempts to send information through this node it may not get back to the master node and the information will be lost. Data loss and integrity is the utmost importance in a network whose sole purpose is to collect and distribute data. Some examples of node failure include being destroyed, tampered with, malfunctioning, and running out of battery.

The last problem that could happen is someone sending bad commands to the motes. Modern sensor nodes can receive commands usually to control some sort of unit. This could potentially be a huge problem is wireless sensor networks that are implemented in places like hospitals.

III. SECURITY IMPLEMENTATION

Implementing security protocols or addressing other security concerns in networks can be complicated but when done correctly, can prove to be very beneficial. One of the best ways to ensure a secure network is to make sure it is implemented correctly. This strategy goes for all networks. If you do not know how to identify a security risk in your code or logic, then you will surely not know how to implement good strategies or patch holes. I would like to go over a few different security methods that researchers have proposed over the past couple of years. I only selected from this period to ensure that they are the most effective on modern WSN's.

authentication keys in security wireless sensor networks. This was first talked about through implementing these methods in a cloud based WSN that could be implemented in a hospital or health care facility. [1] When a life is at stake if security is breached in the network, security is a high priority. Thaier Hayajneh and fellow scientists (names listed in reference [1]) proposed that an authentication method that does not require a lot of processing power should be implemented. The cloud can take care of a lot of the processing done by the local hardware but you still run into some issues with connecting to the network and the amount of traffic if the hospital is large. Cloud aside, this authentication method needs to be lightweight but effective. Thaier Hayajneh and fellow scientists (names listed in reference [1]) proposed that an authentication method that does not require a lot of processing power should be implemented. The cloud can take care of a lot of the processing done by the local hardware but you still run into some issues with connecting to the network and the amount of traffic if the hospital is large. Cloud aside, this authentication method needs to be lightweight but effective.

The Rabin cryptosystem is alike RSA in the fact that it uses the complication of factorials to for its encryption. The Rabin cryptosystem is alike RSA in the fact that it uses the complication of factorials to for its encryption.

to make it far more responsive. to make it far more responsive.

To insure a secure network, this team decided the best practice would be to eliminate the use of smart devices in the sequence. Smart devices, like any device, are susceptible to malware. Likewise, removing them from the group of devices to secure rids of another security concern. The team of researchers decided that the best means of effective encryption would be between the medical staff and the WSN directly. [1:5]

The option that this team chose to use is a method called Rabin encryption. The sensors, in this case, will use a public key to communicate secure information with the main unit and each other when necessary. The public key will be concatenated with additional information to prevent the attacker from generating the code themselves. [1:9] This public key is also used in maintaining data integrity. The data is encrypted with the medical staff's (or smart device's) public key and sent to them so only they can decrypt the information after the request. [1:9]

Before continuing it is worth noting that the Rabin method will not be explained in the paper. To maintain loyalty to the topic I chose and the length requirements it will be excluded. For more information about Rabin encryption please visit *http://www.cs.utsa.edu/~wagner/laws/Rabin.html*.

The researchers conducted an experiment where they could test their version of the Rabin algorithm. In this experiment, they introduced a smart mast node, an actuator node, and an attacker node. [1:20] They tested the encryption times that were a product of the Rabin algorithm and their hypothesis was proven factual and efficient; the modified and parallel Rabin algorithm was a great solution to security in this wireless sensor network. This solution provides a successful encryption key within about 20 seconds, while key authentication takes just under a second. This team concluded that the only power and time consuming task was when the Rabin algorithm had to square the number. Even though it increased energy and time consumption, it was still more effective than its RSA (Originally by Rivest, Shamir, and Adelman) counterparts at using less than half of the energy. The scientists also concluded in their research and experiment that they could add an additional layer of

security by using the public key only for encrypting a private key for transfer but they deemed this unnecessary compared to the additional loss of time and energy. [1:20]

The authentication algorithm that was a modification of the Rabin algorithm that this team implemented for wireless sensor networked proved to be successful. This experiment concluded that this algorithm could be used to insure data integrity, confidentiality, and validity. This security solution also prevented man-in-the-middle attacks and made a way for each segment of hardware to validate itself with each partner device in the communication. [1:23]

Alex Ramos takes a different approach to network security in wireless sensor networks. Ramos proposes that it is not enough to define and implement security in wireless sensor networks, but we must also run evaluations on these security measures. Ramos proposes that information sent through the wireless network should have an estimated security level of how secure it is even in the event of an attack. The level of security that the data has as it arrives at the head unit varies depending on the current state of the network, the path the information traveled, and the original node that sent the data, per Ramos. [2:2106].

A proposition to a fix in security of the wireless sensor networks is the installation of SDSE. SDSE is a software that "communicates with the underlying operating system" to find the security implementations that are already on the network. [2:2107] The uniqueness of this software is that it can detect that a specific (common) implementation of security has not been made and either install if for you or take other actions based on the preference of the operator. A major benefit of SDSE is that the individual sensor nodes do not require any more energy to run this software because it is all ran by the head unit. SDSE also uses a publicly available database to determine whether the hash or encryption algorithms on the network are secure, and how secure they are based on a percent. In [2] it is stated that the database is "publicly available; therefore, such a database can be easily created and distributed along with SDSE."

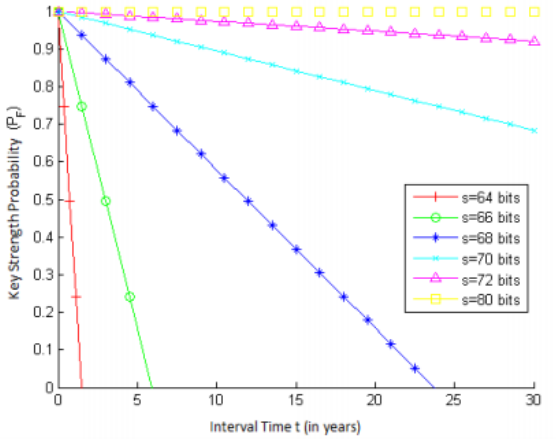
The thing that makes this implementation so interesting is that the calculations are don't in real time. The whole purpose of this application is to let you know that your security is working. It is an interesting proposal because it not only helps you implement security protocols on your network but it will tell you how secure it is with every request; not just on a schedule. SDSE uses two main aspects of network security to determine the security level; prevention and detection. It provides a score on the prevention security model in your network by evaluating the techniques used in defense of your network. This goes into the overall score. The other aspect, detection, is evaluated based on aspects such as whether your network implements effective algorithms to detect intruders and whether your security system rids the network of security problems in a timely manner. [2:2109] This is believed to cover both major aspects of network and node security because it rates both defense and offense.

Testing the efficiency of each of the above categories includes finding the weaknesses of its sub-categories. These sub categories are defined in [2] as "key strength, resilience, and legitimacy." [2:2109] Key strength is determined by the time it would take an attacker program to guess the key based on how big the size of the key generated is. Resilience is determined by the probably of whether the connection that was originally secure, stays secure, and legitimacy is the estimation of the chance that the information

received from the node (or the node itself) is not malicious. [2:2114]

A key aspect of the SDSE software is also rating the intrusion detection system (IDS). As stated earlier, this can be known as the offense of the network. The proposed intrusion detection system proposed in [2] is quite interesting. [2:2114] It proposes a distributive system where the individual nodes work together to identify and isolate malicious nodes. This process is conducted when one node notices suspicious activity in another. Once it notices the suspicious activity, it contacts its neighbors and asks them whether they think that the node is malicious. This is done by generating a binary response from each node. Once all the neighbor nodes have decided, and if the positive amount of decisions equals a certain number, the node that originally detected this unfamiliar activity sends an alarm back to the main unit. [2:2115]

Rating the efficiency of a security measure has many stipulations. It must consider several things of the overall security. The first thing that the SDSE demonstrates is how long it would take to break a security key. As reported in [2] the longer a security key, the stronger and harder it is to break. A graph pulled from this research provides inside to the current lengths based on the RC5 algorithm. [2:2121] *See below*



As demonstrated by this graph, it would take a bit over a year to break a 60-bit key, while if you move it up to an 80-bit key, the time seems unreasonable for a machine to break. Per the report, this graph assumes the secret encryption key has not been compromise. [2:2121]

The paper, conducted by Ramos and Filho (see references for more details) concludes that this is a highly accurate implementation of a security measure in wireless sensor networks. These two conclude that this implementation has approximately a 90% - 100% chance of working efficiently. [2:2135] While they did not want to compare their research to other methods, for the fact that other methods didn't rate their method based on effectiveness, they found that other methods had a lower base accuracy. [2:2136]

IV. CONCLUSION

As wireless sensor networks become more popular over the past years, the concern for security grows. I believe the methods that I researched for this paper, along with a few other papers that I did not have time to include in my research, WSN's have become secure enough to use in important situations like smart cities or hospitals. These networks, though prone to future discoveries and attacks, should be fine to use for whatever purpose you would like and the good news is: most of the methods that I researched are software based and cost very little money to implement.

[1] Thaier Hayajneh, Bassam Mohd, Muhammad Imran, Ghada Almashaqbeh Thaier Hayajneh, Bassam Mohd, Muhammad Imran, Ghada Almashaqbeh, and Athanasios Vasilakos. 2016. Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks. Sensors 16, 4 (2016), 424. DOI:http://dx.doi.org/10.3390/s16040424

[2] Sensor Data Security Level Estimation Scheme for Wireless Sensor Networks. Sensors 14, 1 (2016), 2104 – 2136. DOI:

10.3390/s150102104. Sensors 14, 1 (2016),
2104 – 2136. DOI: 10.3390/s150102104