A Survey of Obstacles and Attacks in Wireless Networks

[1]Mrs.M.Sudha, [2]Dr.S.SavithaDevi

Abstract — As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/computer security. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defenses even harder. We classify the main aspects of wireless sensor network security categories: the obstacles to sensor network security, and attacks.

Keywords — Networks, Sensor, Constraints, Attacks, Security, Cost

— — — — — — — — — — ◆ — — — — — — — — — —

1 Obstacles of Sensor Security

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first.

2 Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

2.1 Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. With such a limitation, the software built for the sensor must also be quite small. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K, and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

Power Limitation Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor The extra power consumed by sensor nodes due to security is related to the processing required for security functions, the energy required to transmit the security related data or overhead and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

3 Unreliable Communications

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. Unreliable Transfer normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key. Conflicts Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be

- [1]*Mrs.M.Sudha, Guest Lecturer Computer Science, Govt. Arts College for Women, Krishnagiri, PH-9159947830, E-mail: sudhamadhaiyan@gmail.com.*
- [2]*Dr.M.S.AvithaDevi, Assistant Professor, Computer Science in Periyar University Constituency College of Arts & Science, Harur. E-mail: savithasanma@gmail.com.*

a major problem. More details about the effect of wireless communication can be found at. Latency The multi-hop routing, network congestion, and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution. Interested readers please refer to on real-time communications in wireless sensor networks.

4 UNATTENDED OPERATION

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes: Exposure to Physical Attacks The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Managed Remotely Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues. Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. No Central Management Point A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

5 ATTACKS

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Denial of service attacks on wireless sensor networks can range from simply jamming the sensor' s communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or any other layer of the wireless sensor network. We note that attacks on wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node' s physical security. In this section, we first address some common denial of service attacks and then describe additional attacking, including those on the routing protocols as well as an identity based attack known as the Sybil attack.

6 TYPES OF DENIAL OF SERVICE ATTACKS

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. This too can have a detrimental impact on the sensor network as the messages being exchanged between nodes may be time sensitive.

6.1 The Sybil Attack

The Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection.

6.2 Traffic Analysis Attacks

Wireless sensor networks are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations. It is not unusual, therefore, for data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an adversary to effectively render the network useless, the attacker can simply disable the base station.

6.3 Node Replication Attacks

Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node replicated in this fashion can severely disrupt a sensor network' s performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor and can also insert the replicated node into strategic points in the network.

6.4 Physical Attacks

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. Recent work has shown that standard sensor nodes, such as the MICA2 motes, can be compromised in less than one 14 minute. While these results are not surprising given that the MICA2 lacks tamper resistant hardware protection, they provide a cautionary note about the speed of a well-trained attacker.

7 Conclusions

Our aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications

References

[1]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks". IEEE Communications Magazine.

[2]. R. Anderson and M. Kuhn. "Low cost attacks on tamper resistant devices". In IWSP: International Workshop on Security Protocols.

[3]. J. Deng, R. Han, and S. Mishra. "Security, privacy, and fault tolerance in wireless sensor networks". Artech House, August 2005.

[4]. G. Gaubatz, J.P. Kaps, and B. Sunar. "Public key cryptography in sensor networks" - revisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[5]. C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures". Elsevier' s AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols.