IJCSC International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 17-19

Wireless Sensor for Effective Network Security Mechanism

P. Felacy Silvia[1], R. Karthiha[2], R. Aarthy[3] & C. Suresh Gnana Das[4]

Final Year Comp. Sci. Engg. [1, 2 & 3] and Professor, Comp Sci. Engg[4]

Vel Tech Multi Tech, Rangarajan, Dr. Sakunthala Engg College, Chennai, India.[1, 2, 3 & 4]

Email: felcysilvia@gmail.com[1], rkarthiha@gmail.com[2], aarthyraviz@gmail.com[3], sureshc.me@gmail.com[4]

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. The deployment of security solutions in Wireless Sensor Networks (WSNs) is considered a challenge due to the highly constrained devices involved in these applications. However, due the need for security services such as confidentiality, integrity and authenticity in a large number of important scenarios, such mechanisms are made necessary.

Keywords: Congestion Control, Wireless Sensor Networks, Security.

1. INTRODUCTION

Wireless sensor networks (WSNs) are an emerging class of networks with a wide variety of potential applications in the fields of health, military and environmental monitoring. Lately there has been an increased focus towards developing transport protocols for WSN's in the research community. While *congestion control* concentrates on enabling the network to recover from packet loss, *congestion avoidance* detects incipient congestion and prevents its occurrence[9]. With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities.

2. OBSTACLES OF NETWORK SECURITY

A wireless sensor network is a special network which has many constraints comparing to the traditional computer network[9].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.

2.1. Limited Resources

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[1]. With such a limitation, the software built for the sensor must also be quite 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 implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered[1].

2. 2. Unreliable 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 [2]. Furthermore, the unreliable wireless communication channel also results in damaged packets

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.

Latency: The multi-hop routing, network congestion, and node processing can lead to the latency of the network, thus make it difficult to achieve the synchronization among sensor nodes[5]. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution[8].

3. UNATTENDED OPERATION

- *Exposure to Physical Attacks:* The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood of a sensor to suffer 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.

- *No Central Management Point:* A sensor network should be a distributed network without a central management point[3]. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

Security Requirements

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements.

1. *DataConfidentiality:* Data confidential-lity is the most important issue in network security[4]. Every network with any security focus will typically address this problem first.
    - A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
    - In many applications nodes communicate highly sensitive data, e.g., key distribution, sothat it is very important to build a secure channel in a wireless sensor network[8].
    - Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks[3].The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.
2. *Data Integrity:* With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray[3]. For example, a malicious node may add some fragments or decrees the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit[9].
3. *Data Freshness:* Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time[7]. However, it takes time for new shared keys to be propagated to the entire network.
4. *Authentication:* An adversary is not just limited to modify the data packet. It can change the whole packet stream by injecting additional packets[5]. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks.
5. *Self-Organization:* Wireless sensor network is a typical ad hoc network, which requires every sensor node be independent and flexible enough to self-organizing and self-healing according to different situations[4]. There is no fixed infrastructure available for the network management purpose in sensor network[2]. This inherent feature brings a big challenge to the wireless sensor network security as well. For example, the dynamics of the whole network inhabits the idea of pre-installation of a shared key between the base station and all sensors[10].

Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notable 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[1] or any other layer of the wireless sensor network.

Due to the potential asymmetry in power and computational constraints, guarding against a well orchestrated denial of service attack on a wireless sensor network can be nearly impossible. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty [2]. 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 take-overs, 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[10].

Defending Measures

Now we are in a position to describe the measures for satisfying security requirements, and preventing the sensor network from attacking. We start from the key establishment in wireless sensor networks, which lays the foundation for the security in wireless sensor network, followed by defending against DoS attacks, secure broadcasting and multicasting, defending against attacks on routing protocols, combating traffic analysis attacks, defending against attacks on sensor privacy, intrusion detection, secure data aggregation, defending against physical attacks, and trust management[9].

*Decentralize Sensitive Data:*The basic idea of this approach is to distribute the sensed location data through a spanning tree, so that no single node holds a complete view of the original data.

*Secure Communication Channel:*Using the secure communication protocols like, SPINS protocols, the eavesdropping and active attacks can be prevented.

Change Data Traffic: Depatterning the data transmissions can protect against traffic analysis. For example, inserting some bogus data can intensively change the traffic pattern when needed.

Node Mobility: Making the sensor movable can be effective to defense the privacy especially on the location. For example, the Cricket system is a location-support system for in-building, mobile, location dependent applications. It allows applications running on mobile and static nodes to learn their physical location by using listeners that hear and analyze information from beacons spread throughout the building[6]. Thus the location sensors can be placed on the mobile device as opposed to the building infrastructure, and the location information is not disclosed during the position determination process and the data subject can choose the parties to which the information should be transmitted.

4. CONCLUSION

In this paper we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, trust, denial of service, and so on . 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. Wireless security faces a number of hurdles, especially the challenge of adapting wireless technologies to work with the mobile world's more constrained resources.

As wireless sensor networks continue to grow, we expect that further expectations of security will be required in wireless sensor network applications.In particular, the addition of public-key cryptography and the addition of public-key based key management will likely make strong security a more realistic expectation in the future..

REFERENCE

[1] "Spec Takes the Next Step ...", http://www.cs.berkeley.edu/~jhill/spec/index.html

[2] J.Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," in *Algorithmic Number Theory (ANTS III),* J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998.

[3] H. Chan, A. Perrig, and D. Song. "Random Key Predistribution Schemes for Sens Networks". *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, p. 197 IEEE Computer Society, 2003.

[4] L. Lazos and R. Poovendran. "Secure Broadcast in Energy-aware Wireless Sensor Networks". *IEEE International Symposium on Advances in Wireless Communications* (ISWC'02), 2002.

[5] Zigbeealliance, 2005, http://www.zigbee.org/.

[6] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant Authentication with Client Puzzles. Revised Papers from the 8th International Workshop on Security Protocols, pp. 170– 177. Springer-Verlag, 2001.

[7] A. Seshadri, A. Perrig, L. van Doorn and P. Khosla. Swatt: Software-based Attestation for Embedded Devices. In Proceedings of the IEEE Symposium on Security and Privacy, May 2004.

[8] S. Rafaeli and D. Hutchison. A Survey of Key Management for Secure Group Communication. ACM Comput. Surv. 35(3):309– 329, 2003.

[9] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: Security Protocols for Sensor Networks. Wireless Networking 8(5):521–534, 2002.

[10] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim. Highly Reliable Trust Establishment Scheme in Ad Hoc Networks. Computer Networks: The International Journal of Computer Telecommunications Networking 45:687–699, Aug. 2004.