

Preface

Wireless sensor network (WSN) is an area of great interest to both academia and industry. It opens the door to a large number of military, industrial, scientific, civilian, and commercial applications. They allow cost-effective sensing especially in applications where human observation or traditional sensors would be undesirable, inefficient, expensive, or dangerous. Wireless sensors have limited energy and computational capabilities, making many traditional security methodologies difficult or impossible to utilize. Also, they are often deployed in open areas, allowing physical attacks such as jamming or node capture and tampering. The threats present to a WSN and the organization of the WSN in response to these threats are influenced directly by the WSN application. As a result, WSN security design and analysis must be sensitive to this context. Otherwise, the assumptions made in the organization of the WSN and the corresponding threats may become inconsistent with the problem domain, leading to solutions that address unrealistic problems.

The security context is not a precise technical specification; rather, it is a set of security-related factors narrowing down the WSN design space to a region that is consistent with them. Clearly, conventional constraints on WSN design, such as cost, form factor, and energy must also be taken into consideration in the technical specification.

As WSN 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. They are exposed to a greater variety of attacks than other networks. The quality and complexity of these attacks are rising day by day. Information transferring through WSN needs to be protected from misuse. Modern security methods need to guarantee safety of data transmission with respect to security needs, i.e., confidentiality, integrity, and availability (CIA). Providing information security in WSN is also necessary, especially for security-sensitive applications and is one of the major concerns addressed in our proposal.

One of the main challenges is the design of these networks and their vulnerability to security attacks leading to network destruction and poor performance. Not only is the quantity and complexity of new threats increasing annually but also the appearance and the momentum. Resistance to them is becoming more and more complicated. Malicious agents are using more of these security vulnerabilities, especially to attack WSN due to the wireless security weakness.

Chapter 2. WSNs are being increasingly used in applications where Quality of Service (QoS) and low cost are the overriding considerations. With increased use, the reliability, availability, and serviceability need to be addressed from the outset. Conventional schemes of using sensor nodes and incorporating these three areas of (reliability, availability, and serviceability) to attain QoS can effectively improve not only the reliability of the overall WSNs, but also the security. We discuss the reverse look of QoS and present mathematically the three significant quality factors that should currently be taken into account in developing WSN application services and security availability, reliability, and serviceability. We also discuss specific characteristics and constraints of WSN, QoS factors when developing security applications for such networks. The security of WSNs has been addressed by providing the flow models and simulations testing using individual sensor nodes on our experiment. To evaluate possibility of establishing secure WSN through QoS, we have used Hawk nodes to demonstrate our approach experimentally. The flow models show how the QoS can be integrated to increase the security of applications running under WSNs.

Chapter 3. We develop mathematical foundations model using the barriers concept to design secure wireless sensors nodes. Security becomes one of the major concerns when there are potential attacks against sensor network nodes. Thus, we have designed fundamental security in disk-shaped to provide basic security elements that can be implemented in various sensor nodes. The mathematical models introduced are flexible and efficient so as to be embedded in sensor nodes and can create a suitable nodes components security in hostile environments.

Chapter 4. In this book, we demonstrated that the complexity of modern attacks is growing. This requires a convergent defensive strategy. Limitations in computation and battery power in sensor nodes constrain the diversity of responsive security mechanisms. We must apply only suitable mechanisms to WSN. Applications of the improved “Feistel Scheme” motivated this approach. The modified accelerated-cipher design uses data-dependent permutations and can be used for fast hardware, firmware, software, and WSN encryption systems. The approach presented shows that ciphers using this approach have less intrusion probability against differential cryptanalysis. This exceeds the currently used popular WSN ciphers such as DES and Camellia.

Chapter 5. Some special features (i.e., resource constraints, impracticality of protecting or monitoring each individual node physically, as well, as their applications normally being supported by many components such as routing and localization) of sensor networks make it particularly challenging to provide security services for sensor networks. We have described a secret distribution scheme (DSS) for sensor networks that achieve automatic secret redistribution. The goal is

to support distributing the secret among new members joining a sensor network without involving a trusted agent or intervention from the user. Our analysis indicates that our new methods have some nice features compared with the previously methods. In particular, the system is efficient. Secondly, it guarantees automatic key distribution after initializations. Thirdly, it does not need urgent key distribution. Finally, it automatically interacts with nodes coalition.

Chapter 6. Current routing protocols in WSNs or even in wireless ad hoc networks are very susceptible to many attacks, i.e., stealthy attack. The most simple among these is where the adversary injects malicious routing information into the network. This results in routing inconsistencies leading to high increase in end-to-end delays or even packet losses in the network. First, we abstract two fundamental routing protocols, which can be generally grouped into two broad categories based on the intrinsic nature of WSN. We argue that none of previous proposed routing protocols satisfies all of them at the same time.

Security in Wireless Sensor Networks

Oreku, G.S.; Pazynyuk, T.

2016, XVII, 87 p. 20 illus., 7 illus. in color., Hardcover

ISBN: 978-3-319-21268-5