A Brief Survey of Access Control in Wireless Sensor Networks

Ismail Butun and Ravi Sankar
Department of Electrical Engineering, University of South Florida, Tampa, FL, USA
e-mails: ibutun@mail.usf.edu, sankar@usf.edu

Abstract—In this paper, we investigate applications of access control to Wireless Sensor Networks (WSNs). Although access control was well established for traditional computer systems, it has not been studied thoroughly in WSN environments. We briefly provide the WSN specifications and then stress the constraints of the WSNs that would affect the access control implementation. We also provide a literature overview and discuss further possible solutions.

Index Terms—wireless sensor networks, security, access control

I. INTRODUCTION

Wireless Sensor Networks (WSNs) continue to grow as one of the most exciting and challenging research areas of engineering. There are many applications of WSNs which are intended to monitor physical and environmental phenomena such as ocean and wildlife, earthquakes, pollution, wild fire, and water quality and also to gather information regarding human activities such as health care, manufacturing machinery performance, building safety, military surveillance and reconnaissance, highway traffic, etc.

WSNs are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. They have unique characteristics such as limited power supplies, low transmission bandwidth, small memory sizes and limited energy; therefore security techniques used in traditional networks cannot be adopted directly. Access control in such a resource constrained WSN with minimum overhead provides significant challenges, and is an ongoing area of research.

The rest of the paper is organized as follows: Section II provides the challenges of access control research in WSNs. Section III reviews related works in the literature. Section IV presents further possible solutions. Finally Section V concludes the paper and outlines future work.

II. CHALLENGES

Access Control provides a solution to confidentiality and it is the key technique to achieve access restriction to the data sources we want to protect. It grants access to legitimate users and denies access to illegitimate outsiders to the WSN data. Since no infrastructure exists in the WSNs, the access control solutions differ from the traditional solutions devised for wireless or wired networks with infrastructure. Providing a unique solution to access control for every application is not possible due to the following challenges in the WSNs:

1) By its nature, WSNs communicate through open air. Therefore it is vulnerable to various kinds of attacks such as eavesdropping, Denial of Service (DoS), man in the middle, etc.
2) The sensor hardware is not reliable, not tamper proof and operates in an unattended environment, which makes it an open target for node capture attacks (physical attack).
3) Even when all the communications between the sensors are properly encrypted and authenticated; access control remains a separate problem to be solved.
4) Secure deployment of new nodes to an existing WSN without the need of renewal of the keys throughout the old nodes is problematic.
5) Revocation of misbehaving nodes from WSN is also a problem to be solved.
6) Sensor nodes are battery powered devices, so energy consumption is very important. Since wireless communication spends much more energy than computing; in order to extend the lifetime of the WSN, any algorithm including communication of the nodes has to be optimized.
7) Providing security with minimum load to the sensor nodes is the main challenge.

III. RELATED WORK

So far, most of the access control schemes proposed for WSNs concentrate on the authentication step of the access control while ignoring the authorization step. The main algorithm considered for this kind of access control (authentication only) is a cryptographic challenge-response protocol, in which a user and network are mutually authenticated to each other.

Defense against node capture is one of the most important yet difficult problems in WSN security, and [1] provides a solution to node capture attacks. Authors propose a framework in which access control to a WSN is achieved by collaboration of a certain number (n) of member sensor nodes. To fulfill the access control operation; the neighboring nodes (n) authenticate and authorize the user who is requesting to participate in the WSN. Although the proposed solution is sufficient to cope with node capture attacks, it increases the communication overhead on sensor nodes, which would cause power supplies of the nodes to deplete rapidly.

[2] presents an energy-efficient access control scheme for WSNs based on Elliptic Curve Cryptography (ECC). Authors propose an energy efficient way to use ECC (which is a Public Key Cryptography (PKC) scheme). The proposed scheme has better performance compared to the other PKC based access control schemes and fair performance compared to Secret Key Cryptography (SKC) based ones. On the other hand, the proposed scheme requires the Key Distribution Center to be available all the time, which may not be the case in some situations and may cause users to be rejected by the access controlling nodes of the WSN.

In [3] authors propose 3 different schemes for WSNs. Proposed schemes have the following advantages compared to existing access control schemes: low expenses in calculation and communication, resistance to node capture, query replay and DoS attacks. On the other hand, the proposed schemes are based on SKC algorithms, which is not scalable compared to PKC algorithms. Besides, in the proposed schemes realizing the privilege control of users is not provided.

In [4] authors propose a dynamic user authentication scheme for WSNs. In the proposed scheme authorized users can access any of the sensor nodes in WSNs which are resource constrained and mobile. The proposed scheme allows legitimate users to query sensor data at any of the sensor nodes in an ad hoc manner. It imposes very little computational load and requires only simple operations. On
the other hand, the proposed scheme is vulnerable to the replay and forgery attacks. Change of passwords is problematic for legitimate users. Passwords could be revealed by any of the sensor nodes.

The proposed scheme of [5] presents a modification to Wong et al.’s scheme [4], that not only fixes the weaknesses but also enhances the security of it. The proposed scheme is resilient against replay and forgery attacks, and it reduces the risk of password leakage from the sensor nodes. It provides users the ability to change their passwords at will. It has better efficiency compared to the previous schemes. On the other hand, the proposed scheme does not provide mutual authentication between the users and the sensor nodes. Besides, it requires a centralized gateway node for registration and password change. Centralized approach may be troublesome for sensor networks; hence most of the currently employed networks do not employ base stations.

In [6] authors propose a distributed user access control under a realistic adversary model in which sensors can be compromised and may collude. Authors propose a practical and scalable certificate-based local authentication based on ECC. PKC eliminates the complicated key management and pre-distribution required by SKC schemes. The proposed scheme is resilient to user collusion attacks. On the other hand, the feasibility of the proposed scheme is questionable. They state that it takes 3.1 seconds to generate a public key and 10.8 seconds to conduct local authentication. These rates are not acceptable in real life, in which a user should be authenticated by the system in less than a second (actually in milliseconds).

In [7] authors implement access control based on ECC on TelosB mote test bed. The security of ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem. Authors provide an application for access control which shows that PKC is feasible to secure WSNs. On the other hand, the proposed access control scheme is vulnerable to impersonation attacks. Besides, the performance of the proposed scheme is poor and it is 80 times more expensive than SKC based access control schemes. The proposed scheme achieves user authentication in 10.1 seconds, which is not acceptable in practical real life applications.

[8] is a tutorial paper comparing SKC and PKC based schemes for access control in WSNs. Their ECC based access control protocol provides pair-wise key sharing between neighboring sensors, local and remote access control. Accordingly they suggest that the PKC based user access control schemes are more advantageous in terms of the memory usage, message complexity, and security resilience compared to SKC based user access control schemes. On the other hand, SKC based schemes are advantageous in terms of computational efficiency.

In [9] authors propose an access control protocol for WSNs based on the ECC algorithm, which prevents malicious nodes from participating in the WSN at the very beginning. Also, key establishment is also included to help new nodes in establishing shared keys with their neighbors. The proposed protocol is resilient against most well-known attacks in WSNs and achieves better computation and communication performance compared to protocols based on RSA algorithm. On the other hand, the usage of PKC in sensor networks is a hot topic of debate and seems it will be so for a while. Unless it is proven, the SKC will be the major tool that will be used for resource constraint sensor networks.

In [10] the author presents an access control scheme based on ECC. The proposed scheme is useful in a sense that it provides a solution to the problem of new node admissions to the WSN which require establishment of keys with the neighboring nodes. On the other hand, the proposed scheme is insecure against replay attacks. Besides it lacks hash chain renewability, causing the WSN to be unusable after the usage of the last key in the hash key chain.

IV. SOLUTIONS

We can use either SKC or PKC for our access control scheme, but we have to know the pros and the cons of each algorithm: SKC based schemes suffer the following problems; they require a large memory to store key materials, provide low scalability due to distribution of the keys, adding and revoking keys is problematic and finally they require complicated key pre-distribution. On the other hand PKC based schemes suffer basically from high energy consumption and considerable time delay. PKC provides a more flexible and simple interface compared to the SKC, which does not require key pre-distribution, pair-wise key sharing or complicated one-way key chain schemes.

Application of PKC is not as easy as first thought. Since the processing power and memory space of the sensor nodes are limited, brilliant solutions are needed for the implementation of the PKC, which will consider the hardware limitations in the design. Secondly the distribution of the certificates for the PKC also needs special attention, which would consider the secure communication protocols between certification authority and users. Thirdly, the SKC needs specific key distribution algorithms and designs, in order to mitigate attacks against the network security. Finally, the security analysis of the overall network should be performed and compared to other existing protocols, which would end up with revision of the design and algorithms.

A novel scheme for user access control in WSNs would bring solutions to the problems addressed above.

V. CONCLUSION AND FUTURE WORK

In this paper we provide a brief literature overview on access control schemes for WSNs. Access control is inevitable when network services are offered to legitimate users only. In this manner, when deploying WSNs, special care must be taken both for the hardware and the software design of the sensor nodes. Depending on the application, the security level of the WSN must be determined and measures should be taken accordingly.

In our future work we will provide more comparative results through software simulations (such as ns-2 or etc.), and resulting outcomes will be published.

REFERENCES


