New Wireless Sensor Networks Security Based on Agents Approach

A.A.BOUDHIR, *MemberIEEE,* M.BOUHORMA, and M.BEN AHMED

Abstract— **Wireless sensor networks (WSNs) have attracted tremendous attention of the research community in recent years. Security becomes one of the major concerns when there are potential attacks against sensor networks. Many services in security, such as authentication and key management, are critical to ensure the normal operations of a sensor network in diverse applications and environments. Thus, familiarity with the current research in this field will benefit researchers greatly. With this in mind, we survey the major topics in WSNs security, and present the main solutions in the sensor security, classify many of the current attacks, We also discuss our proposal architecture based on multi agent platform for ensuring robust security, without key management , in wireless sensor networks with lower energy consumption.**

Keywords :WSN; Energy; Security; Key Management; Agents.

I. Introduction

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. 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 (figure 1).

II. Wireless Sensor Networks Attacks

In order to better understand the security systems that must be able to prevent, counter, detect, and respond to, this section provides a brief overview of sensor network attacks. We note that an attacker may be equipped with either malicious nodes or more sophisticated computing machinery like a laptop or signal generator and signal processing equipment, may be an inside attacker or an outside attacker, or may be a passive or an active attacker. Most trust models assume that the base station is trustworthy as long as it is available.

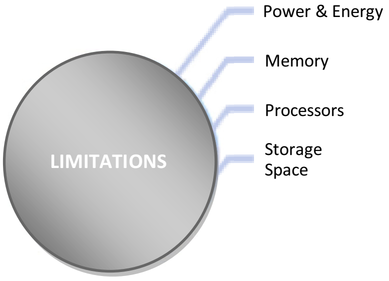

Figure 1: Limited ressources in wireless sensors

Given the great value of the base station, one can argue that it is more likely to be attacked than a sensor. It is also more likely to have network connectivity through a wired or wireless gateway.

Sensor networks are susceptible to attacks starting from the physical layer and going all the way up the stack to the application layer. From the literature [1],[8] the popular sensor network attacks can be classified like mentionned on Table 1.

III. Key Management in Wireless Sensor Networks

In WSNs, most security protocols are based on the cryptographic operations using keys. Key management problem can be de-composed into four phases. The first is the key distribution or pre-distribution phase where secret keys are distributed to sensor nodes for use with the security mechanisms (i.e., confidentiality, authentication and integrity). Sensor nodes have a limited life time, and they are subject to variety of attacks including node capture. New sensor nodes may be deployed and security materials on existing ones may need to be updated. The key management solutions can be classified and evaluated by considering following properties [2]:

- *Underlying network architecture*. In distributed WSN, there is no resource rich member, and sensor nodes have equivalent capabilities. In hierarchical WSN, there are one or more resource rich central stations, and there is a hierarchy among the sensor nodes based on their capabilities.

A.A.BOUDHIR, M.BOUHORMA and the M.BEN AHMED are members of the Computing and Telecommunications Research Group in the Faculty of Sciences and Techniques. Bp416 Tangier Morocco. Respectively their E-mail are : hakim.anouar@ieee.org, bouhorma@gmail.com,med.benahmed@gmail.com.

TABLE I : Popular Attacks in WSN

Sensor Network Attacks	Transport Layer Attacks.
	Software Attacks.
	Key Management Protocol Attacks.
	Network Layer and Routing Layer Attacks
	Physical Layer Attacks.
	Physical Tampering.
	Traffic Analysis Attacks
	Link Layer Attacks.
	Cybil Attack

- *Communication style.* A secure unicast communication between a pair of neighboring nodes requires a pair-wise key shared between them. A reusable pair-wise key is used to secure the unicast communication between more than one pairs of neighboring nodes. Disadvantage is that more than one links are compromised when a reusable pair-wise key is compromised.

- *Key pre-distribution method.* Keys and keying materials are distributed to sensor nodes based on a probabilistic, deterministic or hybrid algorithm.

- *Key discovery and establishment method.* A set of solutions pre-distribute a list of keys, called a key-chain, to each sensor node, and a pair or a group of sensor nodes can secure their communication if they have a key in common.

A. *Key Management in Hierarchical Wireless Sensor Networks*

A Hierarchical WSN (HWSN) includes one or more computationally robust base stations. Sensor nodes are deployed in one or two-hop neighborhood around base stations or resource rich sensor nodes (called cluster heads) as illustrated in Figure 2. Base stations are usually assumed to be trusted and used as the key distribution centers. In a HWSN, pair-wise, group-wise and network-wise keys are required to secure unicast, multicast and broadcast types of communications among sensor nodes, cluster heads and base stations.

- *Pair-wise Key Management*

In a Hierarchical WSN, base station to sensor node, or sensor node to base station unicast communications are secured by using dedicated pair-wise keys. A straightforward approach is to pre-distribute a dedicated pair-wise key to each sensor node so that each base station shares a dedicated pair-wise key with each sensor node deployed within its close vicinity.

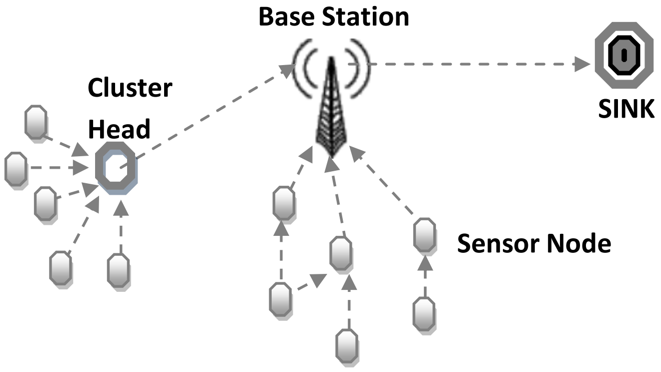

Figure 2 : Hierarchical WSN

- *Group-wise Key Management*

A set of solutions propose to use costly asymmetric cryptography based key management solution. In a HWSN where each base station shares a dedicated pair-wise key with each sensor node deployed within its close vicinity, the base station can intermediate group-wise key establishment. Localized encryption and authentication protocol (LEAP) proposes a group-wise key generation scheme which follows LEAP pair-wise key establishment phase. Assume that sensor node Su wants to establish.

- *Network-wise Key Management*

Network-wise keys are used to secure base station to sensor node broadcast traffic in HWSN. A straightforward but insecure approach is to pre-distribute a single network-wise key to all sensor nodes. Multi-tiered security solution [3] proposes to protect data items to a degree consistent with their value. In key setup phase, each sensor node receives a list of m master keys. Selected master key is named as active master key. RC6 is used as encryption algorithm.

B. *Key Management in Distributed Wireless Sensor Networks*

In a distributed WSN (figure 3), sensor nodes use dedicated pair-wise, reusable pair-wise and group-wise keys to secure their communication, or use keying materials to generate these keys. A part of key management solutions, called key pre-distribution schemes, assign a list of keys, called a key-chain, to each sensor node a priori to the deployment. Others, called key generation schemes, assign keying materials to each node by using which a pair or a group of nodes can generate keys to secure their communication. Solutions to distribute keys and keying materials can be classified as probabilistic [4], deterministic [5], and hybrid [6]. In probabilistic solutions, keys and keying materials are randomly selected from a pool. In deterministic solutions, deterministic processes are used to design the pool and to decide which keys and keying materials to assign to each sensor node so that the key connectivity is increased. Finally, hybrid solutions use probabilistic approaches along with deterministic algorithms to improve the scalability and key resilience.

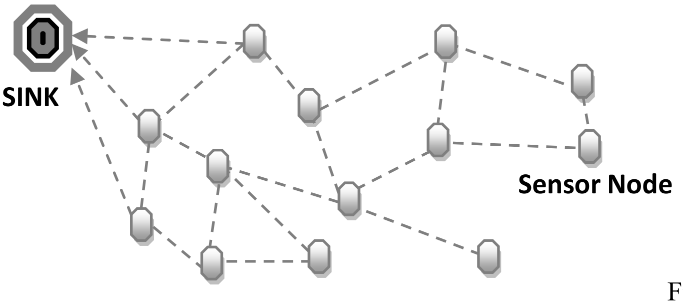

Figure 3 : Distributed WSN

IV. The Agent Security For WSN

A. *Agent Approach*

The agent [7], [9] approach discussed here involves developing a platform Multi agent system ensuring the security of sensors. Indeed, this approach resumed in the ability of agent to manage a set of sensors of its sensing field, taking into consideration a range of sensors, and detects physical intrusion or malicious nodes. These sensors programmed with agents are able to communicate with other sensors. An information report is delivered to the base station (sink) revealing the state of security level of sensors in order to act at time for any outside intrusion. Figure 4 illustrates the key idea of our approach. In this case, the nodes may belong to the same level; the agent ensures the collection in its field of four nodes and returns any anomaly or intrusion to the sink.

B. *Multi Agent Platform*

The pilot implementation of those agents (Sensors) is based on TinyOS component model. TinyOS components are specified using nesC programming language that has a C-like syntax, but supports the TinyOS concurrency model. The main information programmed in modules (to be sensed) is related to movement, exceeding number of sensor belonging to the same fields. Our proposal Multi agent platform is a code containing some data and a control program interpretable on the agent platform. Each platform resides at one sensor and consists of the following modules (figure 5):

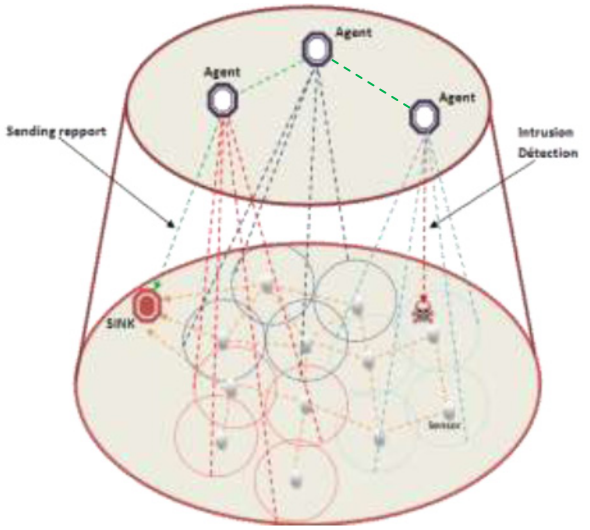

Figure 4: Illustration of intrusion detection approach based on agents

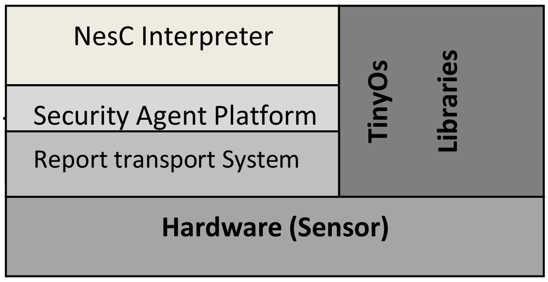

Figure 5: Hierarchy of Platform and agents

- *NesC interpreter*: interpreter of the NesC language that manipulates with agent program and possibly interacts with other modules.
- *Security Agent Platform*: services provided to the agents. It includes computation (a set of functions), interpreter control, when an event or intrusion is received, and it also includes some platform variables that are accessible to particular agents.
- *Report transport system:* responsible of transmission and reporting the security state to the sink.

C. *The Approach Advanteges*

In addition to the security of this architecture, this approach minimizes the energy consumption, needed when processing to distribute and verify keys, compared to other solutions based on cryptography and key management. . Indeed, in this approach, sensors are required to sense with no treatment or management of keys. Therefore, the energy savings can be a result from the implementation of such a platform.

V. Conclusion

This article outlines the usage of key management techniques securing of a wireless sensor network. In add we present a security platform combined with an agent, which is a part of a program code. The computational power for security tasks of a cryptographic key seems greedy on energy whereas the proposal platform reduce this consumption faraway of use the key management.

In the future work we focus firstly on this platform implementation, then to evaluate the energy consumption of the proposal platform with solutions based on cryptography.

REFERENCES

[1] Al-Sakib Khan Pathan, Hyung-Woo Lee, Security in Wireless Sensor Networks: Issues and Challenges, Feb. 20-22, 2006 ICACT2006, ISBN 89-5519-129-4.

[2] Wireless Sensor Network Security, J. Lopez and J. Zhou (Eds.) IOS Press, 2008.

[3] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M. B. Srivastava, On communication security in wireless ad-hoc sensor network, in: IEEE WETICE, 2002, pp. 139–144.

[4] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: IEEE Symp. Security and Privacy, 2003, p. 197.

[5] D. Liu, P. Ning, Location-based pairwise key establishment for static sensor networks, in: ACM Workshop on Security of Ad Hoc and Sensor Netw., 2003, pp. 72–82.

[6] W. Du, J. Deng, Y. S. Han, P. K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in: ACM Conf. Computer and Commun. Security, 2003, pp. 42–51.

[7] Glenn Platt1, The Tiny Agent- Wireless Sensor Networks Controlling Energy Resources, JOURNAL OF NETWORKS, VOL. 3, NO. 4, APRIL 2008

[8] John Paul Walters, Wireless Sensor Network Security: A Survey ©2006 Auerbach Publications, CRC Press

[9] Dimitrios Georgoulas, Intelligent Mobile Agent Middleware for Wireless Sensor Networks: A Real Time Application Case Study, 978-0-7695-3162-5/08 $25.00 © 2008 Crown Copyright.

[10] Peter Pecho, Agent Platform for Wireless Sensor Network with Support for Cryptographic Protocols Journal of Universal Computer Science, vol. 15, no. 5 (2009), 992-1006