PhD Thesis

Subject : Lightweight Cryptography for Autoconfigurable Networks

Directeur de la Thèse : xxx, ***Encadrant :*** Dr. Cherif Diallo

Thèse de l'université Gaston Berger (UFR SAT)
Site internet : http://www.ugb.sn
Département informatique, UFR SAT
Laboratoire ACCA
Université Gaston Berger BP234, Saint-Louis, Sénégal

1. Introduction

The use of MEMS (Micro-Electro-Mechanical-System) technologies has become an integral part of our everyday life. Among the most well-known MEMS technologies today are sensors. Sensors are miniature devices, containing micro-sensors (temperature, pressure, light, presence, etc.), and have extremely limited resources in computation, memory, and energy, as well as a wireless communication interface. The sensors are used in different applications to observe / follow a phenomenon and then transmit its evolution to a central entity (base station, network operator), which will take decisions / actions according to the data collected on the phenomenon.

2. Objectives of the thesis :

In recent years, the use of Wireless Sensor Networks (WSN) has become widespread. The sensors are usually deployed in a region to monitor a phenomenon of interest (temperature, pressure, motion, presence, radiation, etc.), and then trace the events encountered to a base station, which will then make decisions depending on the data collected.

Since sensors are very limited in terms of resource (CPU, storage, energy), compromised, unmanned, and deployable in open and hostile environments, Different types of threats and attacks. Several research work has been carried out to solve security problems related to the WSN, such as: the establishment of sensor pair keys, the security of data aggregation, authentication of a broadcast source, Routing security, as well as access control to the network.

In this thesis, we will try to address three fundamental points in the security of autoconfigurable networks suach that WSN : the establishment of cryptographic keys, the security of the aggregation of the data, and the authentication of a broadcast source. For each of these themes, we will describe the problems involved and then we review the solutions that have been proposed in the literature, analyzing their advantages and disadvantages. Finally, we detail our solutions, and present their advantages compared to existing solutions.

Keywords :
Autoconfigurable network, lightweight cryptography, data aggregation, authentication.

3. References

[1] R. Amin and G. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” Ad Hoc Netw., vol. 36, no. P1, Jan. 2016, pp. 58–80.

[2] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Ranto, “Lightweight cryptography for embedded systems - a comparative analysis,” lNCS, 8247, pp 333-349, 2014.

[3] A. Poschmann, “Lightweight cryptography: Cryptographic Engineering for a PervasiveWorld” PhD dissertation, Ruhr-University Bochum, Germany, February 2009.

[4] C.Bekara, M.Laurent-Maknavicius, "Mitigating Resource-draining DoS attacks on Broadcast Source Authentication on Wireless Sensors Networks ", International Conference on Security Technology (SecTech 2008), published by IEEE CS, Sanya, Hainan Island, China, December 2008.

[5] C. Bekara, M. Laurent-Maknavicius, K. Bekara " H 2 BSAP: A Hop-by-Hop Broadcast Source Authentication Protocol for WSN to mitigate DoS Attacks ", 11 th IEEE International Conference on Communication Systems 2008, IEEE ICCS08, Guangzhou, China, November 2008.

[6] T. Eisenbarth, S. Kumar, C. Paar, and A. Poschmann, “A survey of lightweight cryptography implementations,” Journal IEEE Design & Test archive, Volume 24 Issue 6, Pages 522-533, November 2007.

[7] K. Ren, W. Lou, K. Zeng, and P. J. Moran, “On broadcast authentication in wireless sensor networks,” IEEE Transactions on Wireless Communications, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.

[8] H. Wang, B. Sheng, and Q. Li, “Elliptic curve cryptography-based access control in sensor networks,” Int. J. on Security and Network, vol. 1, no. 3/4, pp. 127–137, Oct. 2006.

[9] K. Piotrowski, P. Langendoerfer, and S. Peter, “How public key cryptography influences wireless sensor node lifetime,” in Proc. of SASN. Alexandria, Virginia, USA: ACM, Oct. 2006, pp. 169–176.

[10] W. Zhang, W. Liu, W. Lou, and Y. Fang, “Securing sensor networks with location-based keys,” in Proc. of IEEE Wireless Communication and Networking Conference. New Orleans, USA: IEEE, Mar 2005, pp. 1909–1914.