Chapter 36
LEAP Enhanced: A Lightweight Symmetric Cryptography Scheme for Identifying Compromised Node in WSN

Maleh Yassine
Hassan 1st University Settat, Morocco
Abdellah Ezzati
Hassan 1st University, Morocco

ABSTRACT

Wireless Sensor Network (WSN) is consisting of independent and distributed sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. The most crucial and fundamental challenge facing WSN is security. Due to minimum capacity in terms of memory cost, processing and physical accessibility to sensors devices the security attacks are problematic. They are mostly deployed in open area, which expose them to different kinds of attacks. In this paper, the authors present an illustration of different attacks and vulnerabilities in WSN. Then the authors proposed a new lightweight cryptography algorithm for identifying compromised node in WSN called Leap Enhanced. Their evaluations on TOSSIM give a precise and detailed idea of the extra cost of consumption of resources needed to ensure the high level of expected security compared to other cryptography schemes in literature.

1. INTRODUCTION

The evolution of wireless communication media has expanded the application fields of sensor networks. Today, WSNs are adopted in a broad range of applications, including surveillance and security, control and automation of production chains, patient surveillance, and fine-grain monitoring. Although it seems that, the sensors have been around for some time, research on wireless sensor networks began in the 1980s, and it is only since 2001 that WSNs generated increased interest from prospects industrial and

DOI: 10.4018/978-1-7998-2454-1.ch036
research (Mayank, 2004). This is due to the availability of low, miniature components cheaply engine such as transformers, radios, and sensors, which are often integrated on a single chip (Huang, 2005).

The different characteristics of sensor networks such as (energy limited, low power calculation, use of radio waves, etc.) expose this type of network to many security threats. Security is one of the crucial challenges in WSN.

Security is the most important issue for WSN and constrained network because of the fact of its application. It can be setup in a very critical system, for example, hospitals, airports, military applications, burglar alarms, environment control, smart homes and traffic surveillance (Maleh, Ezzati, Mbida, & Qasmaoui, 2015).

To deliver security services (integrity, confidentiality, authentication, availability), it is necessary that the communicating nodes share cryptographic keys for encryption and authentication. However, it is well known that the encryption systems represent the first line of defense against all types of attacks. Furthermore, cryptographic techniques must be designed to detect the execution of the most dangerous attacks. In addition, these techniques must be small to fit the limited resources of the WSN (Hegland, et al., 2006).

Sensor networks are highly vulnerable to attacks; it is very important to have certain mechanisms that can protect the network from all kinds of attack. It must be ensured that the system is protected before any kind of attack, during any kind of attacks and after any kind of attack. Cryptographic primitives assure this by allowing authentication of the peers involved in the information exchange. Based on the primitives, it is possible to create better network services. It is also equally important to have a key management system for constructing a secure key infrastructure (Karlof & Wagner, 2003).

Keeping in view the limitations of sensor nodes, a different state of the art algorithms has been studied in depth for the proposal of a key-management scheme based on symmetric shared keys. The two base algorithms for the proposed schemes are “LEAP+” and “improving key negotiation in transitory key schemes”. A straightforward and practical approach for bootstrapping secret keys in sensor networks is predeployed keying. In these schemes, keys are loaded into sensor nodes before deployment.

The unique issue that needs to be considered in sensor network before selecting a key sharing approach is its impact on the effectiveness of in-network processing. The proposed algorithm support in-network processing and also provides security properties similar to those provided by pairwise key sharing schemes.

The critical assumption that LEAP+ has considered is that within Tmin a node cannot be compromised. This hypothesis seems convenient, but only under ideal conditions, it is possible that Tmin is greater than the one assumed. To address this limitation, we propose two models, the first uses a periodic verification “Periodic Chek” to detect the compromised node. The second model executes a sequence number in each node and compared them after the pairwise key establishment step with the information stored in the base station BS, which then makes the decision on whether to delete the shared key (Maleh & Ezzati, 2015).

This work will be organized as well. In the second part, we present the related works. Later, we will discuss and analysis our proposed scheme. We evaluate and we compare LEAP Enhanced with LEAP+ and LEAP++ in terms of connectivity, memory complexity, end-to-end delay, and resistance to attacks. The security analysis was performed on AVISPA tool to gives a precise idea of the efficiency of our scheme. This paper ends with a conclusion.
Related Content

Measuring Dynamics of Ecological Footprint as an Index of Environmental Sustainability at the Regional Level using Geospatial Information Technology: Measuring Ecological Footprint Using GIS
www.igi-global.com/chapter/measuring-dynamics-of-ecological-footprint-as-an-index-of-environmental-sustainability-at-the-regional-level-using-geospatial-information-technology/172717?camid=4v1a

Exact and Efficient Heuristic Deployment in WSN under Coverage, Connectivity, and Lifetime Constraints
www.igi-global.com/chapter/exact-and-efficient-heuristic-deployment-in-wns-under-coverage-connectivity-and-lifetime-constraints/249606?camid=4v1a

Effect of Channel Modeling on Intercept Behavior of a Wireless BAN With Optimal Sensor Scheduling
Deepti Kakkar, Gurjot Kaur, Parveen Kakkar and Urvashi Sangwan (2020). Security and Privacy Issues in Sensor Networks and IoT (pp. 94-124).
www.igi-global.com/chapter/effect-of-channel-modeling-on-intercept-behavior-of-a-wireless-ban-with-optimal-sensor-scheduling/239158?camid=4v1a

CsI and Cs2Te Photocathodes
www.igi-global.com/chapter/csi-and-cs2te-photocathodes/153739?camid=4v1a