Chapter 103
Lightweight Key Management for Adaptive Addressing in Next Generation Internet

Vinod Vijaykumar Kimbahune
Savitribai Phule Pune University, Pune, India

Arvind V. Deshpande
Savitribai Phule Pune University, Pune, India

Parikshit Narendra Mahalle
Savitribai Phule Pune University, Pune, India

ABSTRACT

The continuous evolution of Next Generation Internet (NGI) amplifies the demand for efficient and secure communication capable of responding effectively to the challenges posed by the emerging applications. For secure communication between two sensor nodes, a secret key is needed. Cryptographic key management is a challenging task in sensor networks as the hostile environment of sensor networks makes it more prone to attacks. Apart from resource constraints of the devices, unknown topology of the network, the higher risk of node capture and lack of a fixed infrastructure makes the key management more challenging in Wireless Sensor Network (WSN). Paper surveys different key Management schemes for WSN. The paper presents the efficiency versus security requirements tradeoffs in key management for WSN. Paper also proposes a novel key management protocol which provides strong resistance against replay attacks. The results obtained from the mathematical model based on conditional probability of the scheme suggest that the proposed key management in NGI is efficient and attack resistant.

DOI: 10.4018/978-1-7998-5351-0.ch103

INTRODUCTION

In the context of Next Generation Internet (NGI) everyday devices are globally connected and managing an increasing number of devices requires scalable and efficient addressing mechanism. Due to the economics of scale in NGI, energy, ubiquitous access and secure interaction increases the complexity of operation. Distributed Address Assignment (DAA) proposed by the Zigbee Alliance does not ensure that the device may fail to access and available addresses from its neighbor which is referred as addressing failure. Mobility is another interesting challenge which needs to be addressed essentially in the context of NGI.

Consider a very oboes scenario where frequent travelers carrying NGI compatible device are on tour. Being frequent flyer he can access private and professional information and service through its smart device when he enters into the airport his device should be identified and addressed in the airport context locally. In order to receive different services available in the airport, this operation also involves discovery of public things and services from the smart devices which needs context-aware adaptive addressing. When the traveler roams around in the new and familiar places in city his device needs to find a better route for his journey. In some obvious scenario his smart device also needs to request for guidance to the nearest bus or train stop also there should be a provision where services or other things in the NGI might require user current location which also needs context-aware addressing.

WSN consist of a collection of battery operated sensors which communicate through the wireless medium (Kumar & Nagarajan, 2013). They closely interact with their physical environments and with people, posing new security problems. As the sensor nodes are used in various applications, secure communication between the sensor nodes is needed in order to keep the information secret. A Sensor node sense the information, then processes the information and finally transmits the information in an encrypted fashion to the base station. Cryptographic algorithms will play a vital role in WSN as there are many limitations with respect to the computing power, storage and energy available with these devices. Symmetric cryptographic algorithms are generally more suitable for WSN as compared to asymmetric cryptographic algorithms. Cryptography has mainly two types. Symmetric-key cryptography (SKC) and Asymmetric-key cryptography (AKC) (Parikshit N. Mahalle & Poonam N. Railkar, 2015) (Roy & Dey 2016).

Symmetric-key Cryptography: - In Symmetric-key cryptography, the same key is used for encryption and decryption of the message that is shared secret key. The encrypted message is cipher-text.

1. Figure 1 shows that, User 1 wants to send message (m) to User 2 through the public network by using symmetric key cryptography. They use the same shared secret key (k) to encrypt and decrypt the message.
2. User 1 computes the plain text message c = E (k, m) and sends the encrypted message to User 2 through the public network. User 2 gets the encrypted message c and decode the message D (k, c) = m because of the knowledge of the shared secret key (k).
3. The problem in this communication is that, suppose User 1 repeatedly transmit the message to User 2. Each time they communicate a Trudy (User 3) notice the same cipher-text E (k, m). This is enough for User 3 to derive something from their communication. Where,

m = Message, k = Shared secret key, c = Cipher-text, E = Encryption, D = Decryption