Chapter 11
Security in Network Layer of IoT: Possible Measures to Preclude

B. Balamurugan
VIT University, India

Dyutimoy Biswas
VIT University, India

ABSTRACT

The internet of things (IoT) is an imminent model in the field of wireless telecommunications. It is also considered as a third wave of information technology after the Internet and mobile communication. Basically, IoT is a wireless interconnected network of variety of objects such as radio frequency identification (RFID) tags, sensors, actuators, mobile phones and other types of wireless devices. It has extensible application in the areas such as public security, infrastructure development, modern agriculture, environment protection, urban management, healthcare, enhanced learning, and business service, among others. IoT is a self-configuring wireless network of sensors where the primary goal of establishing connection is to offer interconnectivity of various objects. The concept of IoT was coined by the Auto-Id center of the Massachusetts Institute of Technology (MIT) in 1999

INTRODUCTION

Internet of things (IoT) is an amazing, if not the most powerful technological invention of the last couple of decades, providing superior power to the hands of human race. The most promising aspect of IoT is that this technology is still budding and has immense potential to kick-start a new, fully coordinated technological era. In IoT, 'things' or devices communicate between each other over wireless networks. Therefore, while developing algorithms and techniques for IoT, the standards and rules set for wireless networks, which are essentially different from that of wired networks, are taken into consideration. Since IoT is still in its inception stage, its usage is still limited within the scope of the enterprises and not very common in consumer market. Therefore, unlike the high speed network where computers communicate

DOI: 10.4018/978-1-5225-9866-4.ch011

with other computers where aspects of 'security breaches' is dealt by the programmers and developers for ages, and many robust techniques for this purpose have been built and used, in IoT, with fewer, if not zero, number of cases of security breaches have occurred, apart from standard techniques, it's a challenge for the engineers to develop techniques, both on hardware and software levels, to secure the future of IoT (Kelly et al., 2013; Babar et al., 2010; Alam, Sarfraz, Chowdhury, & Noll, 2011; Barnaghi et al., 2012).

In IoT, the new objects that enter the network are configured automatically. This characteristic makes IoT highly susceptible to security threats. Among several kinds of threats in an IoT network, Disruption and Denial of Service (DoS), eavesdropping, problems in authentication and physical attacks on devices in different forms, are most common.

Therefore, it is essential to devise security measures without interfering with the operation of the IoT network. Also, robust and bug-free analytical tools and algorithms should be employed that will detect malicious and unethical activity, whilst improving service offered to the customers. Generally, the intrusion detection and prevention systems and enhancement of packet security by incorporating suitable fields in packet header are the security measures associated with the Layer 3 of wireless networks (Babar et al., 2010; Zargar et al., 2013; Savola, Reijo, Abie, & Sihvonen, 2012).

SECURITY ISSUES

Ensuring security for the IoT devices has been the most challenging task. Combining a strong cryptography with a highly constrained environment, under the condition of limited energy consumption, since most of the devices are battery operated, and little or no maintenance time makes it extremely difficult. That IoT can achieve intelligent address resolution, track location, monitor and manage devices makes it vulnerable to security threats, as a lot of applications run simultaneously. The security threats commonly found in high speed networks may pose similar menace to IoT, but, in reality, owing to the the low processing power and less storage capacity that are characteristic of devices used in IoT, the protocols designed for higher processing power and greater storage capacity cannot be directly implemented in IoT. With the data moving freely between world wide network of devices, security measures and solutions must be readily available so that users can operate without fear of data manipulation. Therefore, the security measures must be incorporated while designing the device after a proper predictive analysis and not to be treated and adopted for troubleshooting purposes only. At the same time, the choice of security measures should not be made at the cost of compromising users' satisfaction. For the number of intrusion points in a heterogeneous network having billions and possibly trillions of edge devices, the core system requires an equally efficient protection system (Casado, Lander, & Philippas Tsigas, 2009; Babar et al., 2010).

The various security issues that should be provided by a secure network layer for wireless networks are as follows:

1. **Confidentiality:** It ensures that the user information is guarded from unauthorized access. Typically, this is achieved by using symmetric key cryptography for encrypting with a shared secret key. Symmetric key algorithms can be of 2 types, i.e. stream ciphers and block ciphers (Medaglia, Carlo Maria, & Alexandru Serbanati 2010; Weber, 2010).
2. **Semantic Security:** It ensures that no partial information about the plaintext can be extracted by observing the cipher text. A special mode of operation and an initialization vector are often used