Chapter 6
A Rabin Cryptosystem-Based Lightweight Authentication Protocol and Session Key-Generation Scheme for IoT Deployment:
Authentication in IoT

Priyanka Ahlawat
National Institute of Technology, Kurukshetra, India

Ankit Attkan
National Institute of Technology, Kurukshetra, India

ABSTRACT

Handling unpredictable attack vulnerabilities in self-proclaiming secure algorithms in WSNs is an issue. Vulnerabilities provide loop holes for adversary to barge in the privacy of the network. Attacks performed by the attacker can be active or passive. Adversary may listen to the sensitive information and exploit its confidentiality which is passive, or adversary may modify sensitive information being transferred over a WSN in case of active attacks. As Internet of things has basically three layers, middle-ware layer, Application layer, perceptron layer, most of the attacks are observed to happen at the perceptron layer in case of both wireless sensor network and RFID Tag implication Layer. Both are a major part of the perceptron layer that consist a small part of the IoT. Some of the major attack vulnerabilities are exploited

DOI: 10.4018/978-1-7998-6988-7.ch006

by executing the attacks through certain flaws in the protocol that are difficult to identify and almost complex to identify in complicated bigger protocols. As most of the sensors are resource constrained in terms of memory, battery power, processing power, bandwidth and due to which implementation of complex cryptosystem to keep the data being transferred secure is a challenging phase. The three main objectives studied in this scenario are setting up the system, registering user and the sensors via multiple gateways. Generating a common key which can be used for a particular interaction session among user, gateway and the sensor network. In this paper, we address one or more of these objectives for some of the fundamental problems in authentication and mutual authentication phase of the WSN in IoT deployment. We prevent the leakage of sensitive information using the rabin cryptosystem to avoid attacks like Man-in-the-middle attack, sensor session key leakage, all session hi-jacking attack and sniffing attacks in which data is analyzed maliciously by the adversary. We also compare and prove the security of our protocol using proverif protocol verifier tool.

1. INTRODUCTION

Authentication is a procedure of assuring the validity, integrity and trust-worthiness of information. Most basic form of authentication technique is approving the identity/ID of a communicating peer or node, and this ID is provided by the node which has a valid evidence that proves with strong validity that the identity being claimed is correct. The trust among the peers and other communicating pairs of nodes is established by known individuals with their respective verifiable digital IDs that are validated using digital signatures or digital finger-printing.For example, one kind of authentication mechanism is exhibited using the properties and primary attributes to identify digital objects and entities uniquely. In cybersecurity, a human being on a computer node terminal can be denoted as User node which has the privileges only after that individual successfully logs into the computer. According to the level of access provided, the user node has access to resources and data to a certain level. This is where authorization is marked upto a level and the a particular user node has authorized access to only allocated resources and data files access. Root server node is the hub to which network administrator has full access for manipulating, change, deleting or even adding newer data. Large scaled number of IoT edge devices in WSN are not supported by the IPv4, so IPv6 is required which has a wide range of IP addresses. Ipv6 needs a heavy load of battery support and hence making lightweight protocols like ZigBee[1] or 6LowPAN and hash approach based authentication schemes is preferable. Some of the most frequently occurring sensor node attacks in WSNs are node capture attacks[2], smart-card stealth and manipulative forgery attack[3], replay attacks, DOS attacks, session key leakage, user terminal node forgery attack, gateway node (foreign or home does not matter) forgery attack[4], MITM attack etc. Major cause of there adversarial attacks on the wireless sensor networks were an inefficient vulnerable protocol for communication which is unable to authenticate the component nodes of WSN or in simpler terms their cryptographic key generation and maintenance mechanism was not secure enough. By authentication we want to convey the following: i)It is a property that makes sure that an exchange of information is received exactly from