A Survey on Two-Factor User Authentication Schemes in Wireless Sensor Networks

Sharanjeet Kaur
PEC University of Technology
Chandigarh, India

P. Khandnor
PEC University of Technology
Chandigarh, India

***Abstract*— Wireless Sensor Networks have emerged as one of the most promising technologies and promoted research avenues due to their widespread applicability. Wireless Sensor Networks have found applications in critical information infrastructure like military surveillance, nuclear power plants, etc., hence there arises the need to restrict access to critical information of such systems. So as to maintain confidentiality, user authentication is required so that only legitimate users are allowed to retrieve the information. Several two-factor user authentication schemes have been suggested by the research community. In this paper, a brief review of various security issues, security attacks and authentication schemes pertaining to Wireless Sensor Networks has been presented.**

Keywords*— Wireless Sensor Network (WSN), Sensor node, Base station (BS), Gateway node(GWN).*

I. INTRODUCTION

Latest developments in the communication technologies have helped wireless sensor networks (WSN) to emerge as a prominent area of research. A WSN is composed of self-governing sensor nodes which can be installed in hostile environments to measure various attributes like pressure, humidity, temperature, sound, vibration, pollutants, etc. in the surroundings. The sensor nodes have limited computational power, communication range, and storage capacity, so software and hardware platforms, security protocols employed in traditional networks are not applicable to WSNs. WSNs have found applications in the areas of defense, disaster management, traffic monitoring, air quality monitoring, health monitoring, civil engineering, home automation, industrial monitoring, etc. Communication between the nodes takes place via wireless communication channels and they send data collected from the surroundings to the nearby base station (BS)/gateway node (GWN) via multi-hop communication path. Users can retrieve the desired data either from GWN or directly from sensor nodes.

Security maintenance is a major concern in WSNs. Sensor nodes are often deployed in hostile environments, which makes them vulnerable to physical tampering and wireless communication among the sensor nodes facilitates packet injection and eavesdropping. Data confidentiality, integrity and authenticity are primary security concerns to be addressed adequately in WSNs. An efficient user authentication scheme is needed so that only legitimate users are able to retrieve the required information from the network as and when required. The scheme has to be designed keeping in mind their limited computational and communication capabilities.

The paper is structured as: Section II discusses security issues in WSNs and Section III briefly describes two-factor user authentication schemes in WSNs. The two-factor user authentication schemes described in this paper are smart card and password based techniques.

II. SECURITY ISSUES IN WSNS

A. *Security requirements of WSNs*

The primary security concerns for WSNs are as follows [16]:

- Confidentiality**:** It is required so that secrecy of data exchanged between two nodes is maintained. Information exchange related to route updates, location and key management has to be kept secret.
- Integrity: It ensures that data exchanged across the network have not been tampered with.
- Availability: It is required to ensure that there is no jamming of signals or data being transmitted across the network.
- Authentication: It is required so that, the data from the network are extracted by legitimate users only. Users should also be able to ensure that they are receiving data from legitimate sensor node/GWN.
- Freshness**:** It makes the user sure that he/she is receiving the most recent data and previous messages have not been replayed.

B. *Essential Security Features for WSNs*

Various security features required in WSNs are [10]:

- Key agreement: A secret key should be shared between the two communicating entities for encryption of the data to be transmitted, so as to ensure a secure communication.
- Physical Tampering: The attacker extracts secret information like cryptographic keys from the sensor nodes.
- Mutual Authentication**:** Mutual authentication is of prime importance in an authentication scheme. When a user accesses a network, then he needs to ensure

978-1-4799-8047-5/15/$31.00