Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

Advanced password based authentication scheme for wireless sensor networks

Sheetal Kalra [a,*], Sandeep K. Sood [b,1]

[a] Dept. of Computer Science & Engg., GNDU, Regional Campus, Jalandhar, India
[b] Dept. of Computer Science & Engg., GNDU, Regional Campus, Gurdaspur, India

ARTICLE INFO

Article history:
Available online 4 November 2014

Keywords:
Authentication
Complex networks
Smart card
Wireless sensor networks

ABSTRACT

This era of ubiquitous computing has led to the development of complex communication networks all over the world. Wireless sensors, due to their wide applicability, form a key component of any complex network. But, security is a major challenge in making wireless sensor networks robust. Many remote user authentication schemes have been proposed for authenticating the legitimate users of a wireless sensor network. Most of the recently proposed schemes are vulnerable to one or more security attacks and are inefficient in terms of processing time. In this paper, the scheme proposed by Xue et al. has been reviewed and it has been found that the scheme is vulnerable to impersonation attack, stolen smart card attack, server spoofing attack. This paper proposes a robust and efficient password based authentication scheme which is secure against all well known security attacks. Moreover, the scheme has a low computation and communication cost and does not suffer from time synchronization problem. A formal security analysis has been performed using AVISPA tool to prove the security of the protocol.

1. Introduction

Wireless sensor network (WSN) is an emerging technology that shows great potential for various futuristic applications, both military and civilians. A wireless sensor network is a collection of sensor nodes organized into cooperative networks. The basic idea of sensor networks is to disperse tiny sensing devices which are capable of sensing variations in specific parameters related to a particular application and communicating with other devices in the network. The sensing technology combined with processing power and wireless communication makes an ideal choice for many applications in defense as well as public. This new technology has unlimited potential for applications in the area of military, transportation, entertainment, medical, homeland defense etc. Sensor networks usually interact with sensitive data and operate in hostile environments where the communication over WSN is subjected to various security threats. Therefore, network security is a desirable requirement for the successful implementation of such networks. Wireless sensors technology also holds great application for Internet-of-Things (IoT). In 2012, Ning and Hu (2012) described the role of sensors in future IoT.

In 2012, Xue et al. (2012) proposed a temporal credential based mutual authentication and key agreement scheme for wireless sensor networks. The scheme provides mutual authentication between the user, sensor node and gateway

* *Corresponding author.* Tel.: +91 9357314576.
E-mail addresses: sheetal.kalra@gmail.com (S. Kalra), san1198@gmail.com (S.K. Sood).
[1] Tel.: +91 9465204534.

http://dx.doi.org/10.1016/j.jisa.2014.10.008

node (GWN). In this paper, the scheme proposed by Xue et al. (2012) has been analyzed and it has been found that their protocol is vulnerable to impersonation attack, server spoofing attack and stolen smart card attack. In addition to this, the protocol has other weaknesses like impractical assumption and incorrect login phase. This paper proposes an efficient remote user authentication scheme for wireless sensor networks using smart cards. Sensors and smart cards are small electronic devices with limited resources and need such authentication protocols which are not only secure but also cater to severely resource constraint environment of a wireless sensor network. Authentication protocols based on static identity schemes leak out the partial information about the user thus again leading to compromise of the scheme (Yeh et al., 2010; Cheng et al., 2006). On the other hand, in dynamic identity schemes the identity of the user changes with every login and even if the attacker launches a replay attack by recording various communication messages, he fails to login as a legitimate user. The protocol operates under the assumption that the smart is tamper-resistance.

The scheme proposed in this paper has the following merits: **1)** The protocol is based on the concept of dynamic identity and is immune to replay attack; **2)** The concept of dynamic identity is implemented using nonce values so there is no time synchronization problem; **3)** The protocol has a low computation and communication cost; **4)** It prevents offline dictionary attack even if the information stored in the storage device is compromised; **5)** The identity of the user changes dynamically for every new session; **6)** It achieves mutual authentication between the three communicating viz. the user, sensor and GWN; **7)** It provides two factor authentication using GWN and smart cards; **8)** All well known attacks are prevented using our protocol.

2. Communication architecture

In a typical Wireless Sensor Network (WSN), a gateway node GWN is used to communicate the information of a particular application between the sensor node and outside world and vice versa. The communication between the sensor node, gateway node and other communicating devices must be implemented using secure and efficient authentication protocols. The three communicating entities viz. user of the network, the sensor node and the gateway, must mutually authenticate each other before processing any request for data (Fig. 1).

In complex wireless sensor network, hundreds or thousands of sensor nodes are randomly deployed over a certain area of interest. One of fundamental goals for wireless sensor networks is to collect information from the physical world where sensor nodes sense the physical phenomenon, process it and send the data to the environment via gateway node. The gateway node helps to connect to an external network such as Internet. Communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of threats. Typical sensor nodes are small with limited communication and computing capabilities and are equipped with limited power source and in some cases replenishment of power sources may not be feasible. In WSN, the energy consumption can be categorized based on sensing, communication and data processing. The lifetime of the WSN will be increased if the energy consumption is reduced. The security protocols devised for traditional networks cannot be directly applied on such networks because in comparison with traditional computer networks, wireless sensor networks work in constrained computational and energy resources. Applying encryption/decryption techniques devised for traditional networks require transmission of extra bits hence need extra processing memory and battery power which are the most critical resources for the sensor's longevity. Due to these power constraints, it is impossible to directly employ the existing security approaches to a WSN. All security approaches require certain amount of resources including data memory, code space and processing power for implementation. Thus, the challenge is to devise such security protocols which are capable of maximizing the processing capability and energy reserves of WSN while securing them against attackers.

3. Related work

In last few years, a number of schemes have been proposed for authenticating remote users of a wireless network. In 2004, Watro et al. (2004) proposed a public key cryptography based authentication protocol for sensor networks. But their protocol was computationally inefficient as it was based on RSA and Diffie-Hellman algorithms which involve complex mathematical equations. In 2009, Das (2009) found that the scheme proposed by Watro et al. (2004) and was insecure against user masquerading, Replay and sensor spoofing attack. In 2007, Wong et al. (2007) proposed a less complex dynamic user authentication protocol which was based on symmetric cryptographic parameters of hash function. In 2009, Das (2009) found that the schemes proposed Wong et al. (2007) were vulnerable to replay, forgery and stolen verifier attack. He proposed a two factor authentication scheme for wireless networks involving GWN architecture. The schemes provided a password authenticated solution based on hash function and XOR operation for resource constrained environment of sensor networks. Although the scheme was computationally efficient but it did not provided mutual authentication and session key agreement. In 2010, He et al. (2010) and Khan and Alghathbar (2010) improved the scheme proposed by Das (2009). The improvements made by He et al. (2010) were not very significant as those done by Khan and Alghathbar (2010). The later had improved the scheme of Das (2009) by using the hash value of the password instead of direct password and providing mutual authentication among GWN and sensor node. The scheme proposed by Khan and Alghathbar (2010) had the limitation of storage lookups for GWN and incorrect password updating procedure. In 2010, Chen and Shih (2010) proposed an authentication scheme which provides mutual authentication among the user, GWN and the sensor node but the scheme is vulnerable to forgery and replay attack. Recently, a few authentication schemes based on ECC have also been proposed by the researchers. In 2011, Yeh et al. (2011) proposed an ECC based remote user authentication scheme. The computational cost of the protocol was high as