Ad Hoc Networks 36 (2016) 58–80

Contents lists available at ScienceDirect

Ad Hoc Networks

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

A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks

Ruhul Amin*, G.P. Biswas

Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, India

ARTICLE INFO

Article history:
Received 20 October 2014
Revised 21 May 2015
Accepted 28 May 2015
Available online 19 June 2015

Keywords:
Authentication
Security Attacks
WSNs

ABSTRACT

Wireless sensor networks can be deployed in any attended or unattended environments like environmental monitoring, agriculture, military, health care etc., where the sensor nodes forward the sensing data to the gateway node. As the sensor node has very limited battery power and cannot be recharged after deployment, it is very important to design a secure, effective and light weight user authentication and key agreement protocol for accessing the sensed data through the gateway node over insecure networks. Most recently, Turkanovic et al. proposed a light weight user authentication and key agreement protocol for accessing the services of the *WSNs* environment and claimed that the same protocol is efficient in terms of security and complexities than related existing protocols. In this paper, we have demonstrated several security weaknesses of the Turkanovic et al. protocol. Additionally, we have also illustrated that the authentication phase of the Turkanovic et al. is not efficient in terms of security parameters. In order to fix the above mentioned security pitfalls, we have primarily designed a novel architecture for the *WSNs* environment and basing upon which a proposed scheme has been presented for user authentication and key agreement scheme. The security validation of the proposed protocol has done by using *BAN* logic, which ensures that the protocol achieves mutual authentication and session key agreement property securely between the entities involved. Moreover, the proposed scheme has simulated using well popular *AVISPA* security tool, whose simulation results show that the protocol is *SAFE* under *OFMC* and *CL-AtSe* models. Besides, several security issues informally confirm that the proposed protocol is well protected in terms of relevant security attacks including the above mentioned security pitfalls. The proposed protocol not only resists the above mentioned security weaknesses, but also achieves complete security requirements including specially energy efficiency, user anonymity, mutual authentication and user-friendly password change phase. Performance comparison section ensures that the protocol is relatively efficient in terms of complexities. The security and performance analysis makes the system so efficient that the proposed protocol can be implemented in real-life application.

1. Introduction

A wireless sensor networks *(WSNs)* typically consist of low cost, low power, large number of sensor nodes which are deployed manually or randomly over the target region. *WSNs* have become an emergent and popular technology for its potential applications in environmental monitoring, agriculture, health care, disaster management, domestic and surveillance systems [1]. At first it was thought that the wireless sensor networks would be only homogenous, that means all the sensor nodes are identical in terms of power, capability etc. But, presently the infrastructure of *WSNs* could be

* Corresponding author. Tel.: +91 8804152340.
E-mail addresses: amin_ruhul@live.com, ruhulamin@cse.ism.ac.in, ruhulamin.hit@gmail.com (R. Amin), gpbiswas@gmail.com (G.P. Biswas).

http://dx.doi.org/10.1016/j.adhoc.2015.05.020
1570-8705/

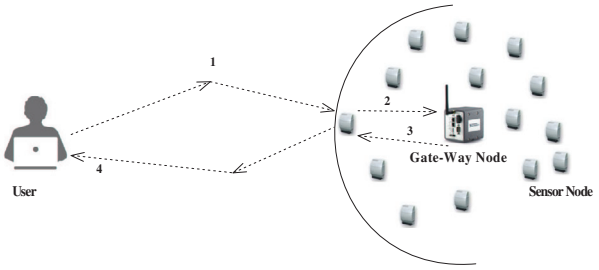

Fig. 1. Turkanovic et al.'s architecture.

heterogenous consisting of different capabilities. In this paper, we have assumed that the network model is heterogenous wireless sensor networks in which all the sensor nodes sense the desired data and forward to the nearby gateway node directly and the user outside the network can access the sensed data to fulfill their objectives. As the messages are transmitted through insecure networks, the attacker/adversary can intercept, insert, delete, re-route the communicating messages. Therefore, several security aspects such as user authentication, message integrity along with privacy are the foremost concern for such type of network model. In order to provide secure communication over the insecure channel, a session key agreement protocol between the entities involved is necessary, where the mutual authentication as well as user anonymity property are highly important. To design an efficient user authentication and key agreement protocol for the *WSNs*, the following security aspects should be achieved:

1. An efficient login phase is necessary so that the protocol can detect wrong input information(s) in the early stage.
2. An authentication phase should be efficient in terms of computation and communication complexities.
3. Resistance of off-line password guessing attack.
4. Resistance of off-line identity guessing attack.
5. Resistance of user-impersonation attack.
6. Resistance of server masquerading attack.
7. Mutual authentication property between all the entities involved in the system.
8. The protocol should resist session key computation attack.
9. The protocol should provide perfect forward secrecy.
10. Resistance of insider attack.
11. Resistance of replay attack.
12. Avoidance of clock synchronization problem.
13. Password/identity/biometric change phase should be provided and to be efficient if applicable.
14. The computation, communication and storage cost should be as minimum as possible.
15. Session key agreement.
16. As the energy of the sensor nodes are very limited, so the energy consumption should be as minimum as possible.
17. In the authentication phase of the proposed protocol, the gateway node should be performed more computation than the sensor node to increase the lifetime of the networks.

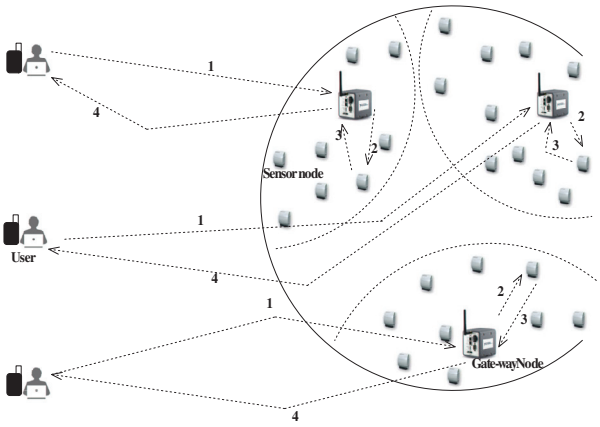

Fig. 2. Multi-gateway based proposed protocol architecture of the WSNs.

1.1. Energy model

In *WSNs*, the sensor nodes are powered by small batteries and recharging or replacing the batteries may not be always possible, as the sensor nodes are deployed in hostile environment for many applications. Although it is a challenging task, but for the prolonged network service, the energy conservation specially of the sensor nodes of the *WSNs*, is mandatory. The main components of a sensor nodes are a microcontroller, transceiver, external memory, power source and one or more sensor(s), where the transceiver is responsible for transmitting and receiving the messages. As mentioned in [2], Eq. (1) is used to measure the energy consumption for transmitting *l-bits* message over a distance (d) and similarly, the energy consumption equation for receiving the *l-bits* message has presented in Eq. (2), where free space model(fs) is used when the distance (d) is less than a threshold value d_0; otherwise, multi-path (mp) model is used.

$$E_T(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & \text{for} \quad d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 & \text{for} \quad d \geq d_0 \end{cases} \tag{1}$$

$$E_R(l) = lE_{elec} \tag{2}$$

where E_{elec} is the energy required by the electronic circuit, ε_{fs} and ε_{mp} be the energy required by the amplifier in free space and multi-path model respectively.

The above discussion clearly confirms that the communication cost of the sensor node depends on transmitting and receiving the l-bits messages and also directly proportional to the distance between the sensor nodes and the target entity. Therefore, the minimum distance between the gateway node and the sensor node should be desirable property of the *WSNs* model for reducing power consumption. It is well-known that the gateway node has high energy resources and can efficiently communicate to the desired entities.

1.2. Network model and comparisons

The network model of the Turkanovic et al. and the proposed protocol are presented in Figs. 1 and 2 respectively. Like Turkanovic et al.'s, the proposed model also consists of three types of entities such as (a) sensor nodes, (b) gateway