ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city

Xiong Li [a,*], Jianwei Niu [b,*], Saru Kumari [c], Fan Wu [d], Kim-Kwang Raymond Choo [e]

[a] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China

[b] State Key Laboratory of Virtual Reality Technology and Systems, School of Computer Science and Engineering, Beihang University, Beijing 100191, China

[c] Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India

[d] Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China

[e] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

HIGHLIGHTS

- Weaknesses of a previous authentication scheme for GLOMONET are pointed out.
- Requirements of authentication for GLOMONET in smart city are summarized.
- A robust three-factor authentication scheme for GLOMONET in smart city is proposed.
- Security analysis and comparisons with other related schemes are illustrated.
- Analysis and comparison results show our scheme is robust for smart city environments.

ARTICLE INFO

Article history:
Received 29 November 2016
Received in revised form
20 March 2017
Accepted 7 April 2017
Available online xxxx

Keywords:
GLObal MObile NETwork (GLOMONET)
Smart city
Authentication
User anonymous
Biometrics

ABSTRACT

Smart city is a development tendency of future city, which improves almost all aspects of quality of urban residents' life by adopting Information and Communication Technology. In smart city, people can interact directly with the community and the infrastructure at anytime and anywhere, where GLObal MObility NETwork (GLOMONET) is an important network infrastructure for smart city. Recently, Gope and Hwang proposed an efficient authentication scheme for GLOMONET. However, we find their scheme lacks session key update and wrong password detection mechanisms, and vulnerable to denial-of-service attack. Besides, the session key can be known by *HA* (home agent), and perfect forward secrecy cannot be ensured. Furthermore, in their scheme, *HA* has to take heavy secret key management work. Based on previous work, this paper first summarizes the security and function requirements of authentication for GLOMONET in smart city environment. Later, this paper proposed a robust biometrics based three-factor authentication scheme for GLOMONET in smart city. Security features of the proposed scheme are analyzed in detail, and comparisons of our scheme with other related schemes are illustrated. Analysis and comparison results show that our scheme meets the preconcerted security requirements of authentication for GLOMONET in smart city environment, and it is robust for GLOMONET in smart city environments with higher security requirements.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Smart city [1] is a new urban development vision to improve all aspects of urban residents' life quality by integrating various information techniques, such as big data, cloud computing [2–5] and Internet of Things. By using smart city technologies, people could build series so-called smart environments, such as smart home, smart library, intelligent transportation system, smart healthcare, and precision agriculture. These smart environments allow user to enjoy smart services [6,7] at anywhere. Ubiquitous network access is an important foundation for these smart city applications since network is a crucial pipeline for data transmission in these smart city applications. GLObal MObility NETwork (GLOMONET) plays a vital role in development of smart

* Corresponding authors.
E-mail addresses: lixiongzhq@163.com, lixiong84@gmail.com (X. Li), niujianwei@buaa.edu.cn, niujianwei2008@gmail.com (J. Niu), saryusiirohi@gmail.com (S. Kumari), conjurer1981@gmail.com (F. Wu), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

http://dx.doi.org/10.1016/j.future.2017.04.012
0167-739X/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: X. Li, et al., A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.04.012

city, which provides roam services for mobile user, and makes mobile user access network anywhere. Generally, there are three types of participants in GLOMONET, i.e. mobile user (*MU*), home agent (*HA*) of *HA*'s home network and foreign agent (*FA*) of a foreign network. First, a *MU* registers at *HA*, and then *MU* can access services even if he/she roams into a foreign network (or *FA*) beyond the scope of *HA*'s jurisdiction. Since the open characteristic of wireless channel, GLOMONET is full of attacks since it attracts more adversaries' attention. Therefore, security and privacy protection become a major challenge of GLOMONET in smart city.

Authentication is a basic and easy implement mechanism to guarantee information security in network applications, and it is widely used in almost all information systems. Based on a path breaking study [8] on user authentication via insecure channel, many authentication schemes are designed by researchers for different environments, such as e-health [9], and wireless body area networks [10,11]. Generally, there are three types of elements used for authentication, i.e., password, hardware equipment such as smart card, and biometrics. With the increasing attack ability of adversaries, new means of network attacks emerge in endlessly. Single factor based user authentication schemes [12–14] have been unable to cope with some business with high security requirements, such as in mobile payment and smart healthcare. Later, multi-factor authentication schemes [15,16] are proposed.

In GLOMONET, authentication is also an important mean to guarantee the security of the system, which allows *FA* authenticates a *MU* with the help of *HA* before *MU* accesses to *FA*. In 2004, Zhu and Ma first proposed a user authentication scheme with anonymity for wireless environments [17]. However, Lee et al. [18] found that the scheme of [17] is vulnerable to forgery attack and failed to achieve mutual authentication, and they designed an improved scheme to remedy the weaknesses. Later, Wu et al. [19] pointed out that both Zhu and Ma's scheme [17] and Lee et al.'s scheme [18] cannot protect user anonymity well. In 2009, Chang et al. [20] showed that the scheme in [18] is incapable of offering the feature of user anonymity, and they proved that a malicious mobile user of a *HA* can gain other users' identities who had registered at a same *HA*. To remove the weaknesses of Lee and Hwang's scheme [18], Chang et al.'s [20] also proposed an improved scheme. Unfortunately, their scheme was found unable to provide anonymous features [21] as well. In 2009, He et al. [22] proposed a strong user authentication scheme for GLOMONET. There scheme is suitable for power limited devices since their scheme just needs to perform symmetric cryptographic algorithm and hash operation. However, Li and Lee [23] found some flaws of scheme in [22], i.e. their scheme lacks user friendless, cannot provide unlinkability of a user, and the session key can be predetermined by *MU*. To remedy these weaknesses, Li and Lee [23] proposed an enhanced scheme for GLOMONET based on the intractability of Diffie–Hellman problem. In 2011, Yoon et al. [24] designed an anonymous authentication scheme for wireless communication using digital certificates. However, Niu and Li [25] pointed out that their scheme cannot provide fair key agreement, and the sessions from a special user can be traced by an adversary. In 2013, Jiang et al. [26] proposed a user authentication scheme with privacy preserve for GLOMONET based on quadratic residue assumption. However, Wen et al. [27] found the scheme in [26] is vulnerable to stolen-verifier attack and replay attack, and they proposed an improved scheme for GLOMONET. Unfortunately, Gope and Hwang's work [28] shows that offline guessing attack and forgery attacks are feasible to the scheme in [27]. Later, many authentication schemes for GLOMONET have been proposed to enhance security or improve efficiency. Recently, Gope and Hwang [29] also pointed out some weakness of the scheme in [22], and they proposed an improved scheme. Really, symmetric cryptographic and hash operations make Gope and Hwang's scheme [29] is efficient for GLOMONET environment. However, their scheme is unpractical due to the following weaknesses: their scheme lacks verification mechanism for wrong password and would be vulnerable to denial-of-service (DoS) attack; their scheme lacks a session key update mechanism and the session key shared between *MU* and *FA* can be known by *HA*; their scheme cannot ensure perfect forward secrecy of session key as they claimed; *HA* needs share a secret key with each mobile user, and *HA* would undertake heavy key management work. In this paper, we first summarize the security and function requirements of a user authentication for GLOMONET in smart city, and then a robust three-factor user authentication for GLOMONET in smart city has been proposed based on bilinear pairing.

The rest of this article are as follow: Section 2 introduces some preliminaries used in this paper. Review and cryptanalysis of the scheme in [29] are given in Section 3. The proposed scheme, the formal proof, and the corresponding security features are presented in Sections 4, 5 and 6, respectively. Our scheme is compared with related schemes in Section 7, and the conclusion is given in Section 8.

2. Preliminary knowledge

This section introduces some basic knowledge, contains the universal adversary model used in this paper, security and function requirements of user authentication scheme for GLOMONET in smart city, basic information about biometrics fuzzy extractor and bilinear pairing.

2.1. Adversary model

Based on previous work [30–32], we assume that an adversary $\mathcal{A}$ has the following capabilities, and it will be used to evaluate the security features of smart card based authentication schemes.

1. $\mathcal{A}$ has control of the public communication channel among three parties, i.e. he/she can intercept, modify, replay, insert and delete any message in the public channel.
2. $\mathcal{A}$ may steal user's smart card and extract the parameters in it by using the methods in [33,34].
3. $\mathcal{A}$ may be an insider of the system, and may intercept the registration request parameters of users'.
4. $\mathcal{A}$ is familiar with the protocol working and environment variables such as public parameters.

2.2. Security and function requirements

Based on previous work, we summarize following security and function requirements of a security and practical user authentication for GLOMONET in smart city:

1. **Quickly detection of wrong password**. Generally, people may be involved in many different network based applications, therefore user usually needs to manage a large number of identity and password pairs, and may input a wrong password when he/she login to the system. Therefore, a wrong password detection mechanism is desirable for user authentication that the validity of user's password could be verified at smart card/mobile device. With this mechanism, session initiated by wrong password would quickly rejected by mobile device, and it would save a lot of computational and communication cost.
2. **Mutual authentication**. In the user authentication for GLOMONET in smart city, *MU* can access *FA*'s services when the validity of *MU* is verified by *FA* with the help of *HA*. For security consideration, mutual authentication should be achieved among *MU*, *FA* and *HA*, and it can avoid many attacks, such as man-in-the-middle attack and forgery attack.

Please cite this article in press as: X. Li, et al., A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.04.012

Download English Version:

https://daneshyari.com/en/article/6873179

Download Persian Version:

https://daneshyari.com/article/6873179

Daneshyari.com