A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks

Guangquan Xu, Jia Liu, Yanrong Lu, Xianjiao Zeng, Yao Zhang, Xiaoming Li

PII: S1084-8045(18)30040-7

DOI: 10.1016/j.jnca.2018.02.003

Reference: YJNCA 2062

To appear in: *Journal of Network and Computer Applications*

Received Date: 16 August 2017

Revised Date: 25 December 2017

Accepted Date: 2 February 2018

Please cite this article as: Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y., Li, X., A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.02.003.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

A Novel Efficient MAKA Protocol With Desynchronization for Anonymous Roaming Service in Global Mobility Networks

Guangquan Xu, Jia Liu, Yanrong Lu*, Xianjiao Zeng, Yao Zhang, Xiaoming Li
*: Tianjin Key Laboratory of Advanced Networking (TANK), School of Computer Science and Technology,
Tianjin University, Tianjin, China 300350

***Abstract*-In the roaming service system of Global Mobile Networks (GLOMONET), mutual authentication and key agreement (MAKA) protocol is used to identify legitimate roaming users and establish a secure session between users and servers. In recent years, many MAKA protocols are proposed. Among them, the most representative is Gope-Hwang's, which uses the low-cost cryptographic primitives, and hence is more suitable for battery-powered mobile devices. In this paper, we analyze the deficiencies of Gope-Hwang's protocol and propose a novel efficient MAKA protocol with desynchronization for anonymous roaming service in GLOMONET. Gope-Hwang's protocol is lightweight but is susceptible to replay attacks and have a large storage burden. We utilize symmetric encryption to implement dynamic random pseudo-ID, which can achieve anonymity, solve storage burden problem and reach desynchronization. Informal analysis and automated security validation with AVISPA Tool show that our protocol can resist many common attacks such as replay attack, lost smart card attack, forgery attack etc. Moreover, compared to the other four selected protocols in our performance analysis, the efficiency of our protocol outperforms all the other work and is increased by 9.6% than that of Gope-Hwang's.**

***Keywords*—Anonymity, Authentication, Global Mobility Networks (GLOMENTS), Roaming service, AVISPA**

1. Introduction

The rapid development of mobile networks has greatly facilitated people's lives. When a user moves from one place to another, Global Mobility Network (GLOMONET) ensures that a travelling wireless device is kept connected to network without breaking the connection (Chaudhari and Biradar, 2016; Du et al., 2017). With the help of the home agent, Global Mobility Network (GLOMONET) can identify legitimate users and allows legitimate mobile users to use roaming service anytime anywhere. The model of wireless roaming network is shown in fig. 1. However, data transmission in mobile network is vulnerable to various attacks, especially replay attacks, which can result in many security risks, such as loss of user privacy data, system paralysis and so on. Hence, it is necessary to design a secure mutual authentication and key agreement (MAKA) protocol. In order to ensure the privacy of users, anonymous communication (Artail and Abbani, 2016) in GLOMONET is an imperative issue. In addition, due to the limited computing ability of mobile devices, it requests the protocol must be efficient and lightweight (Li et al., 2017).

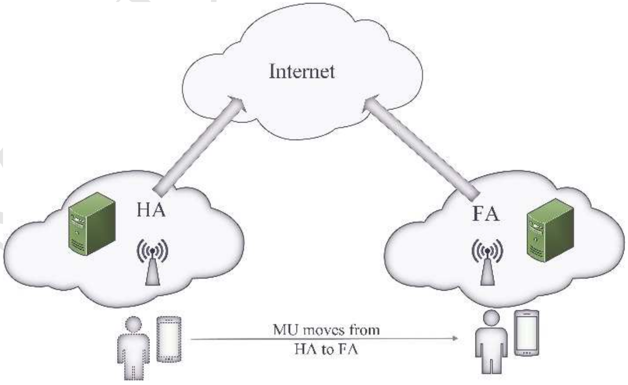

Fig. 1. The model of wireless roaming network.

1.1. Related work

Over the past years, many MAKA protocols for the GLOMONET have been proposed. In 2006, Lee et al. (Lee et al., 2006) proposed a new authentication scheme with anonymity for wireless environments. However, in the paper of Wu et al. (Wu et al., 2008) it was shown that the scheme by Lee et al. fail to provide user anonymity, and they proposed an enhanced scheme by providing an effective remedy. Independently, Yoon et al. (Yoon et al., 2011) proposed a user friendly authentication scheme with anonymity for wireless communications. Unfortunately, Li (Li, 2012) found that the scheme designed by Yoon et al. is vulnerable to insider attack and fails to achieve user anonymity. Based on Yoon et al.'s protocol, Li proposed a more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. However, Kai et al. (Kai et al., 2016) showed that the scheme designed by Li suffers from replay attack and DDoS attack. Besides, Li's scheme does not clearly explain how to obtain corresponding session keys and the relationship between different users so that Li's scheme lacks integrity. And