Computer Networks 99 (2016) 66–81

Contents lists available at ScienceDirect

Computer Networks

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

GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications

Chengzhe Lai[a,b,*], Rongxing Lu[c], Dong Zheng[a,*], Hui Li[b], Xuemin (Sherman) Shen[d]

[a] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China
[b] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, China
[c] School of Electrical and Electronics Engineering, Nanyang Technological University, 639798, Singapore
[d] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

ARTICLE INFO

Article history:
Received 20 November 2015
Revised 11 January 2016
Accepted 3 February 2016
Available online 12 February 2016

Keywords:
Machine to machine (M2M)
Machine-type communications (MTC)
Group authentication and key agreement
Security
Lightweight
The 3rd generation partnership project (3GPP)

ABSTRACT

Supporting a massive number of machine to machine (M2M) devices has been considered as an essential requirement in M2M communications. Meanwhile, cyber security is of paramount importance in M2M; if M2M devices cannot securely access the networks through efficient authentication, all applications involving M2M cannot be widely accepted. One of research challenges in M2M is group authentication since a large number of M2M devices accessing the network simultaneously will cause a severe authentication signaling congestion. To solve this problem, as well as reduce authentication overhead of the previous schemes based on public key cryptosystems, we propose a novel lightweight group authentication scheme for resource-constrained M2M (GLARM) under the 3GPP network architecture, which consists of two protocols that can achieve efficient and secure group authentication in the 3GPP access case and non-3GPP access case, respectively. GLARM can not only authenticate all M2M devices simultaneously, but also minimize the authentication overhead. The security analysis shows that the proposed scheme can achieve the security goals, and prevent the various security threats. In addition, performance evaluation demonstrates its efficiency in terms of computation complexity and communication overhead.

1. Introduction

Machine-to-machine (M2M) communications [1], also named machine-type communication (MTC) [2], which is standardized by the 3rd generation partnership project (3GPP). M2M is an emerging technology empowering full mechanical automation (e.g., in the smart grid, smart transportation, etc.), and its rapid development will change our living styles vigorously. The M2M technology is drawing overwhelming attention in the standardization and industry areas, which has been actively engaged in by many standards forums and organizations, including IEEE, European Telecommunications Standards Institute (ETSI), Third generation partnership project (3GPP) and 3GPP2. Among them, the 3GPP MTC has been regarded as the promising solution facilitating M2M communications [3].

With the development of M2M technology, the requirements of efficiency, reliability and security (GRS) are being paid more attention by mobile network operators and research groups [4]. For *efficiency*, low power M2M devices have been highly attractive in many scenarios due to the

* Corresponding authors. Tel.: +86 13468922875.
E-mail addresses: lcz_xupt@163.com, lcz.xidian@gmail.com (C. Lai), rxlu@ntu.edu.sg (R. Lu), zhengdong@xupt.edu.cn (D. Zheng), lihui@mail.xidian.edu.cn (H. Li), sshen@uwaterloo.ca (X. (Sherman) Shen).

http://dx.doi.org/10.1016/j.comnet.2016.02.007
1389-1286/

fact that they can be deployed in a wide range of applications and easily retrofitted, thus significantly reducing installation costs. Moreover, thousands of low power M2M devices can work unattended for years, hence they need to be deployed and maintained at a very low cost. However, many traditional communication protocols cannot be applied to these resource-constrained M2M devices since they introduce too much overhead.

Cyber security is also of paramount importance in M2M communications; if M2M devices cannot securely access the networks through efficient authentication, all applications involving M2M cannot be widely accepted. However, the recent authentication and key agreement (AKA) protocols dedicated for 3GPP Evolved Packet System (EPS), known as EPS-AKA [5]; or for non-3GPP access networks (e.g., WLAN or WiMAX), known as EAP-AKA [6] cannot provide enough security [7–10]. In addition, to support M2M communications, the 3GPP mobile operator has to accommodate its network to support a large number of MTC devices, which can overload its network resources and introduce congestion in the network at both the data and control planes [11]. In fact, congestion may occur due to simultaneous authentication signaling messages from M2M devices. For instance, if a group of M2M devices detect a base station, they send their access authentication requests toward the core network at the same time, leading to congestion in the different nodes of the network, across the communication path. If a large number of M2M devices in a group need to access the network simultaneously, the traditional authentication protocols (e.g., EPS-AKA or EAP-AKA) will suffer from high signaling overhead, leading to authentication signaling congestion and decreasing the Quality of Service (QoS) of the network. The reason is that every device must perform a full AKA authentication procedure with the home authentication server, respectively. Considering *reliability*, these traditional AKA protocols are not suitable for large-scale M2M communications.

In order to speed up the process of authentication and avoid authentication signaling congestion in group-based communications, some batch verification schemes based on bilinear pairing have been proposed, such as [12–14], etc. Although these schemes can effectively authenticate a group of devices at the same time, they may not be suitable for resource-constrained devices, because the communication is an “expensive” resource due to its effect on the battery life of resource-constrained devices and the bandwidth of the channel. To fulfill the requirements of efficiency, reliability and security, a more efficient group authentication protocol dedicated for M2M devices in 3GPP networks is desirable.

In this paper, we focus on the problem of group AKA for resource-constrained M2M devices in 3GPP networks. On one hand, to address the issue of authentication signaling congestion, the core network needs to authenticate all M2M devices in a group at one time; on the other hand, the novel protocol should aim to reduce the authentication overhead in previous schemes. Therefore, we propose a lightweight group authentication scheme for resource-constrained M2M in 3GPP networks to achieve these goals. The proposed scheme can authenticate all MTC devices simultaneously based on aggregate message authentication codes (MACs). In addition, the proposed scheme considers both 3GPP access and non-3GPP access cases. The main contributions of this paper are as follows:

(1) We propose a novel group-based lightweight authentication scheme for resource-constrained M2M (GLARM) under the 3GPP network architecture, which consists of two protocols that can achieve efficient and secure group authentication in the 3GPP access case and non-3GPP access case, respectively. In addition, our scheme is developed based on the 3GPP standard and thus can be compatible with the 3GPP standard protocols.
(2) GLARM fills security requirements in previous protocols. Moreover, it can successfully resist some sophisticated attacks, such as redirection [8], man-in-the-middle attacks [7], etc. GLARM can implement mutual authentication and key agreement between multiple M2M devices and the core network simultaneously. Meanwhile, the network congestion because of mass M2M device connections can be avoided in the 3GPP networks and the QoS requirements can be guaranteed.
(3) Due to hardware-limited resources, the low-cost computation and communication authentication scheme is required. Since public key cryptosystems usually execute more computations, we adopt symmetric cryptosystems to reduce the computation cost. Furthermore, the number of round trips between M2M devices and the core network is reduced, which decreases the communication cost.

The remaining of this paper is organized as follows. In Section 2, we preview the related works. In Section 3, we introduce our network architecture, security and design goals. In Section 4, we present our GLARM, followed by its security analysis and performance evaluation in Sections 5 and 6, respectively. Finally, we draw our conclusions in Section 7.

2. Related works

There have been many research works on authentication and key agreement protocol in 3GPP networks.

For 3GPP access network (e.g., UMTS, LTE or LTE-Advanced), in 2005, Zhang and Fang [9] point out that 3GPP AKA has some security weaknesses. The first weakness is that it is vulnerable to a variant of false base station attack, which allows an adversary to redirect user traffic from one network to another. The second weakness is that it allows an adversary to use the authentication vectors (AVs) corrupted from one network to impersonate the other networks. The third weakness is that the use of synchronization between a mobile station (MS) and its home network (HN) incurs resynchronization. To overcome these weaknesses, Zhang and Fang propose an improved authentication and key agreement protocol called AP-AKA.

In 2010, Ou et al. [15] propose Cocktail-AKA to overcome the congenital defects of UMTS-AKA. Cocktail-AKA