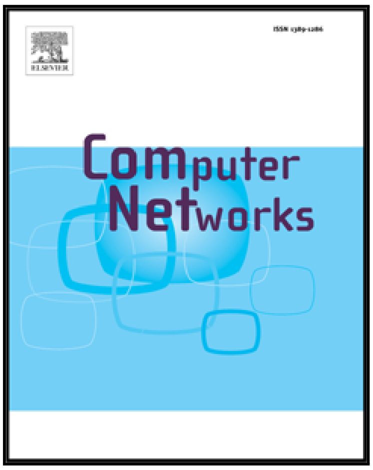
An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems

Yue Qiu , Maode Ma , Shuo Chen



PII:	S1389-1286(17)30381-X
DOI:	10.1016/j.comnet.2017.10.006
Reference:	COMPNW 6321

To appear in: *Computer Networks*

Received date:	3 May 2017
Revised date:	29 September 2017
Accepted date:	18 October 2017

Please cite this article as: Yue Qiu , Maode Ma , Shuo Chen , An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.10.006

An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems

Yue Qiu, Maode Ma and Shuo Chen
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

Abstract—The Internet has made our planet a smaller world while the cyber world and the physical world have not been integrated seamlessly. In the future cyber-physical system (CPS), all objects in the physical world would be connected to the cyber world for achieving faster information processing, more accurate control and real-time response. Our abilities of controlling facilities and handling events will be much more powerful to make our lives much better. In the CPS, the machine-to-machine (M2M) communication, which is in charge of data collection, utilizes both wireless and wired systems to monitor environmental conditions and transmits the information among different systems without direct human intervention. As a part of the CPS, the M2M communication is considerable important while being fragile at the same time since M2M communication still faces lots of security threats. There are some security vulnerabilities that yet to be solved. In this paper, we propose an anonymous authentication scheme for multi-domain M2M environment. The proposed scheme applies hybrid encryption scheme involving certificateless cryptography and advanced encryption standard (AES) to achieve the authentication and anonymity properties. The security analysis with Burrows–Abadi–Needham (BAN) logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA) shows that the proposed scheme is well designed and could withstand multiple attacks, such as Man-in-the-Middle attacks, replay attacks, DoS attacks, impersonation attacks and compromised attacks.

Keywords—Authentication; M2M; Multi-Domain; Anonymous

1 Introduction

With the rapid development of communication technology, the emerging CPS is going to connect all of the objects in the physical and cyber world [1]. In the future, each object in the world will be uniquely identifiable and their virtual representations will be an Internet-like structure. CPS is an integrated part of future Internet which aims to establish a dynamic network of billions or trillions of identifiable objects communicating and interacting with each another for real-time data collection, analysis and better decision making. The objects could be physical sensors/devices or a digital entities/services that have identities, attributes and intelligent interfaces to be seamlessly integrated into the Internet through interoperable communication protocols. Over the CPSs, the connected objects can report their locations and states and are able to exchange information among each other automatically without human’s operation.

There are three major types of the components to form the three tiers in a CPS [2]. One type of the components is a group of sensing devices to form an environmental tier. The second type is the actuator, which can form a service tier. And the last type is the controller forming the control tier. The sensing devices collect information from the physical system and then send the information to the network which is handled by the distributed controllers in the cyber world. After processing the information, the controllers communicate with the actuators to issue appropriate operation commands. Then, the actuators will act to impose the physical world through activating the related operations and generate feedback. Based on the closed process of sensing, decision, execution and feedback, the CPS can achieve self-awareness, self-judgment and self-adjustment [3]. The environmental tier of CPS is formed by the M2M communication system to collect physical information for data analysis. An M2M communication system consists of three interlinked domains: 1) A sensing domain including sensing devices with M2M gateways, 2) A network domain including wired/wireless networks and 3) An application domain consisting of the end users and applications required in the CPS [4].

The M2M communication network in a CPS has a few weaknesses which make the system unsecured [5-6]. First of all, the M2M communication system is easy to be eavesdropped. Secondly, the sensing devices or gateways, which are normally unattended, could be compromised by attacker stealthily. Lastly, the integration of wireless and wired medium may be incompatible and could be a potential threat. So it is very important to construct an effective security scheme against various attacks to protect the M2M communication system.

To address the security of M2M systems, some authentication schemes [7-17] have been proposed to ensure the secure network connection with a legitimate M2M device. Moreover, some group-based authentication schemes for M2M devices [18-22] have also been proposed. However, most of the proposals focus on the