Chapter 10

Machine-to-Machine Communications and Security Solution in Cellular Systems

Mahdy Saedy
University of Texas at San Antonio, USA

Vahideh Mojtahed
Purdue University, USA

ABSTRACT

This paper introduces an efficient machine-to-machine (M2M) communication model based on 4G cellular systems. M2M terminals are capable of establishing Ad Hoc clusters wherever they are close enough. It is also possible to extend the cellular coverage for M2M terminals through multi-hop Ad Hoc connections. The M2M terminal structure is proposed accordingly to meet the mass production and security requirements. The security becomes more critical in Ad Hoc mode as new nodes attach to the cluster. A simplified protocol stack is considered here, while key components are introduced to provide secure communications between M2M and the network and also amongst M2M terminals.

1. INTRODUCTION

Conventional telecommunication networks enable Human-to-Human (H2H) communications characterized with fairly high demand for bandwidth to accommodate for the voice and data applications. The total low cost of ownership, fast network rollout and numerous capabilities of wireless data networks can bring the machine-to-machine communication known as M2M to a wider audience and exceedingly broad and diverse application scenarios. M2M is a special type of communication where the majority of end user terminals are entities that communicate with each other and interact with the environment without human intervention in terms of collecting data and taking required actions based on received commands from the network. Large number of communicating terminals, small and infrequent traffic has already generated numerous market scenarios leading to developing the supervisory control and data acquisition (SCADA) systems in the early 1990s, based on technology in which a

DOI: 10.4018/978-1-4666-2154-1.ch010
centralized server reaches out and polls field equipment regularly. SCADA is based on proprietary technologies, so its costs never dropped enough to make widespread deployment practical. Unlike SCADA, M2M system works with standard technologies such as TCP/IP, IEEE wireless/wired LANs, and cellular technologies. Using standards allows easier device interoperation in M2M systems and provides scalable network expansion with less expensive and quicker implementation while the total cost of ownership is lower due to mass-production of M2M terminals. With the advent of new and smart applications, the need for higher data rate and ubiquitous coverage as well as the ability for M2M terminals to interconnect and expand regardless of network limitations, where needed, is well understood. In other words, today’s M2M communications needs to be defined on modern wireless platforms like 4G with Ad Hoc capability. 3GPP LTE-Advanced standards can deliver the required data rate and QoS for this purpose while we also consider Ad Hoc scenario to enable the M2M terminals to interact with each other where they succeed to form a local Ad Hoc cluster within the coverage of 4G system. Enhanced QoS, mobility and resource management along with high bit rate for fixed and mobile users in 4G system, opens new horizons to M2M communications.

Security is one of the most critical issues in networks which are well established for H2H communications in 3GPP standards. For M2M terminals to be able to form Ad Hoc cluster within the coverage of 4G cellular networks, it is extremely important to revisit the security procedures since machines can interact with other machines in Ad Hoc mode as well as normal access to 4G network resources.

2. CONVENTIONAL M2M SOLUTION

Figure 1 shows a typical wireless M2M implementation based on 2G system (GSM) via protocols such as TCP/IP. The system sends the information to a back-end server, which processes the data and sends it via the Internet to a monitoring center that monitors and controls the machines.

In current networks, the M2M terminal acts similar to a normal mobile phone, which communicates with the base station and then with the M2M server via the upper layer (i.e. NAS in 3GPP). The difference might be that the machine is triggered by a specific event other than human being (Chen & Yang, 2009). The actual data to be sent may be of very small volume due to successive handshakes with the network. These transmissions and extra overheads cause power waste which makes the current system not economic for M2M communications (Cristaldi, Faifer, Grande, & Ottoboni, 2005).