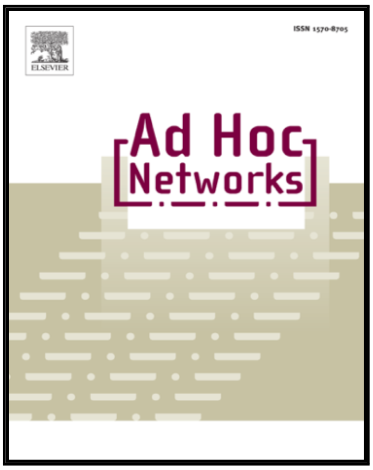
A Policy-aware Service Oriented Architecture for Secure Machine-to-Machine Communications

Georgios Katsikogiannis , Dimitrios Kallergis ,
Zacharenia Garofalaki , Sarandis Mitropoulos , Christos Douligeris



PII: S1570-8705(18)30312-3
DOI: 10.1016/j.adhoc.2018.06.003
Reference: ADHOC 1687

To appear in: *Ad Hoc Networks*

A Policy-aware Service Oriented Architecture for Secure Machine-to-Machine Communications

Georgios Katsikogiannis, Dimitrios Kallergis, Zacharenia Garofalaki, Sarandis Mitropoulos, Christos Douligeris
Department of Informatics, University of Piraeus, Greece
{gkatsikog, d.kallergis, z.garofalaki, sarandis, cdoulig}@unipi.gr

Abstract

Breakthrough recent advancements in the field of machine-to-machine (M2M) communications impose the necessity to improve the service delivery by enforcing appropriate security rules. Due to the large number of the connected devices, the criticality of the M2M applications (e.g. patient monitoring and operation of critical infrastructures), and the network stability weaknesses, we need to consider and analyse the security aspects and establish a flexible policy-aware Service Oriented Architecture (SOA) competent to deal with these emerging challenges. This paper presents the existing reference models and proposes a novel Secure M2M Architecture (SeMMA) based on ETSI's M2M communication functional architecture enhanced with policy-based management capabilities and SOA capabilities. We explore the policy-based management aspects to improve the security of the M2M components and services and to mitigate the security concerns that arise by evaluating different scenarios. It is shown that incorporating an adaptive policy enforcement of the suitable security controls enables enhanced security capabilities, increased agility, and better service levels in the field of M2M communications.

Keywords–*M2M communications; security policies; SOA; service domain; policy enforcement*

1. Introduction

In the last few years, several applications (e.g. transportation, human/inventory tracking, water/energy distribution and quality monitoring, personal area and home and habitat networking and monitoring, data centre monitoring, disaster avoidance and recovery, military surveillance and industry operations, medical/healthcare monitoring, process monitoring and smart spaces) rely on the capabilities of the machine-to-machine (M2M) communications. These applications collect the environmental/physical information and conditions from the M2M measurement nodes and process, analyse and present the measurement data. Several security and service quality issues arise due to *(a)* the high number of interconnected heterogeneous smart objects, *(b)* the use of various networking technologies for the M2M communications, and *(c)* the distributed nature of the smart applications into consideration. These interconnected objects are resource-constrained devices in respect to power-consumption, computational capabilities, bandwidth and storage capacity [1]. Concerning the network communication protocols, the M2M environments need to support cross-domain information exchanges among several smart interconnected nodes. Because of the distributed and dynamic nature of the environment, the M2M nodes are free to move, trigger a high rate of physical topology changes, and operate in an unattended fashion with very limited maintenance support. These fundamental M2M characteristics complicate the operations of the routing and management protocols, the M2M communication services, the device reachability, and raise various security issues [2].

To achieve an effective use of M2M applications and improved service levels, we need to identify the service requirements and then efficiently manage the available constrained resources. In this vein, the policy-based management allows the creation of policy expressions and afterwards enables the policy enforcement. The benefits of the policy-based management approach arise as the M2M