computer
communications

TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications

Fayez Alqahtani, Zafer Al-Makhadmeh, Amr Tolba, Omar Said

PII: S0140-3664(19)31245-9
DOI: https://doi.org/10.1016/j.comcom.2019.11.030
Reference: COMCOM 6032

To appear in: *Computer Communications*

Received date : 24 September 2019
Revised date : 13 November 2019
Accepted date : 19 November 2019

Please cite this article as: F. Alqahtani, Z. Al-Makhadmeh, A. Tolba et al., TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications, *Computer Communications* (2019), doi: https://doi.org/10.1016/j.comcom.2019.11.030.

TBM: A Trust-Based Monitoring Security Scheme to Improve the Service Authentication in the Internet of Things Communications

Fayez Alqahtani[1], Zafer Al-Makhadmeh[1], Amr Tolba[1,2,*], Omar Said[2,3]
[1]Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia.
[2]Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin-El-Kom 32511, Egypt.
[3]College of Computers and Information Technology, Taif University, Taif, Saudi Arabia.
*Corresponding Author: atolba@ksu.edu.sa

Abstract
Securing communications and information sharing within the Internet of Things (IoT) paradigm is challenging because of the increase in the size and mobility of the user population. Moreover, managing a central security architecture requires adaptability and integration with a cloud network. In this manuscript, a trust-based monitoring (TBM) scheme was designed for improving the security features in cloud-assisted IoT environments. This security scheme employs middleware and intelligent agents for managing user- and communication-level security. TBM operates in three security administering phases namely spoof detection, trust construction, and message authentication. The intelligent agents are responsible for ensuring secure communication by exchanging trust and signal strength observations with the middleware. These agents also assist with monitoring, processing, and task switching to reduce communication costs. TBM was evaluated through extensive simulations. The results demonstrate its consistency in achieving lower response and detection times, misdetection probabilities, and false positive rates. In addition, it was found to improve network lifetime through reduced energy consumption.

Index Terms—Agent Technology, Attribute Monitoring, Middleware, Secure Communication, Trust Assessment, IoT.

1. Introduction

The Internet of Things (IoT) is one of the wireless technology improvements that enable device-to-machine (D2M) and machine-to-machine (M2M) communication through a common network. The components include smart real-world devices and their virtual representations, information and communication technologies (ICTs), services, applications, processing units, and storage. The basic building block in the IoT is the end-user device that possesses smart sensing, actuating, transducing, and storage-assisted computing capabilities [1,2]. The network is modeled to access, to process, and to share heterogeneous information to meet the application demands at the beneficiary level. Information is gathered from multiple wired and wireless connected sources that are stored and processed as digital information for D2M or M2M communication [3,4]. With the integration of automation, sensors, and electro-mechanical devices with smart means of communication, the IoT applications are far-reaching. They are used in areas such as health care, the environment, environmental monitoring, and intelligent transportation services. The physical, virtual, and ICT components and services have improved the utilization, adaptability, and flexibility of IoT networks and devices [5,6].

Communication in the IoT is developed by connecting smart devices through the internet. This presents challenges, such as mobility, interoperability, scalability, security, and privacy, that must be addressed. Security is a major concern because device- and service-level authentication is essential for confronting the emerging cyber-physical attacks [7–9]. The increased security threats to the internet and the current issues in sensor networks must be simultaneously addressed to improve data confidentiality, authentication, and integrity in the IoT. The security deployments