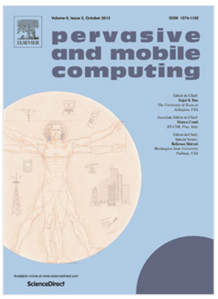
Journal Pre-proof



Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks

Floriano De Rango, Giuseppe Potrino, Mauro Tropea, Peppino Fazio

PII: S1574-1192(19)30470-5
DOI: https://doi.org/10.1016/j.pmcj.2019.101105
Reference: PMCJ 101105

To appear in: *Pervasive and Mobile Computing*

Received date : 30 November 2018
Revised date : 12 October 2019
Accepted date : 14 October 2019

Please cite this article as: F. De Rango, G. Potrino, M. Tropea et al., Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks, *Pervasive and Mobile Computing* (2019), doi: https://doi.org/10.1016/j.pmcj.2019.101105.

Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks

Floriano De Rango[a], *Giuseppe Potrino[a], Mauro Tropea[a], Peppino Fazio[a]

[a]*University of Calabria, DIMES Department, P. Bucci 39/c, 87036 Rende (CS), Italy*

Abstract

Security in the context of Internet of Things (IoT) is a critical challenge. The purpose of this work is to model and evaluate a dynamic IoT security system based on a generic IoT edge network in which nodes exchange messages through the Message Queue Telemetry Transport (MQTT) protocol. This work aims to increase MQTT security by mitigating data tampering, eavesdropping and Replay attacks by using the Elliptic Curve Cryptography (ECC),timestamps and wake up patterns, with the purpose of preserving node energy. The evaluated results will show that it is possible to increase the system lifetime by linking security levels and energy.

Keywords: IoT, ECC, MQTT, Replay attacks, IDS

1. Introduction

The term IoT was born as a title of a presentation made by Kevin Ashton in 1999 at MIT [1]. IoT overlaps between Mobile Computing, Pervasive Computing, Wireless Sensor Networks and Cyber Physical System. IoT can be defined as a wired or wireless network constituted by connected and unequivocally identified devices able to process data and communicate with each other with or without human help. Nowadays, the IoT is used in many fields for example: Logistic, Smart environment, Smart Agriculture, Smart citiesetc. By the end of 2020 it is estimated that there will be approximately 30 billionconnected devices with a data exchange greater than 40 Zettabytes

*Corresponding author. Floriano De Rango, e-mail: derango@dimes.unical.it
Authors e-mail addresses: giuseppe.potrino@unical.it(G. Potrino), derango@dimes.unical.it (F. De Rango), m.tropea@dimes.unical.it (M. Tropea), p.fazio@dimes.unical.it (P. Fazio)