Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks

Khizar Hameed, Abid Khan, Mansoor Ahmed, Goutham Reddy Alavalapati, M. Mazhar Ullah Rathore

PII: S0167-739X(17)32275-6
DOI: https://doi.org/10.1016/j.future.2017.12.009
Reference: FUTURE 3847

To appear in: *Future Generation Computer Systems*

Received date : 3 October 2017
Revised date : 21 November 2017
Accepted date : 3 December 2017

Towards a Formally Verified Zero Watermarking Scheme for Data Integrity in the Internet of Things based-Wireless Sensor Networks

Khizar Hameed[a], Abid Khan[b], Mansoor Ahmed[b], Goutham Reddy Alavalapati*[c], M. Mazhar Ullah Rathore[d]

[a]*Department of Computer Science, University of Management and Technology, Sialkot, Pakistan*
[b]*Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan*
[c]*Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea*
[d]*School of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea*

Abstract

The Internet of Things (IoT) is an emerging paradigm in which billions of devices communicate, thus producing and exchanging information related to real world objects (things). Sensor nodes are specialized nodes for handling transmission of a large volume of data in situations where the source nodes communicate with base stations (BS) via a set of intermediate nodes. Applications based on WSN claim that integrity and trustworthiness are the key aspects as the data received from source nodes is the major source for BS to take critical decisions. To establish the trustworthiness between sensor node and BS, a novel zero watermarking scheme is proposed in this paper. In order to ensure integrity and trustworthiness, our proposed scheme embeds a watermark in original data before it is transmitted to BS which is responsible for verifying the watermark embedded with data. We have compared proposed scheme with existing Asymmetric Cryptography (ACT) and Reversible Watermarking (RW) schemes based on the performance parameters such as computational overhead and the energy utilization. Analysis results suggest that proposed scheme can handle multiple attacks on data and watermark such as data deletion, data modification, and data insertion attack. Moreover, our experimental results demonstrate that the presented scheme is lightweight, computationally efficient, and better in energy utilization. A formal verification for proof of correctness using high level Petri nets (HLPNs) is also provided to verify the claims of our work.

Keywords: `Zero Watermarking, Data integrity, Sensor networks, High level petri nets(HLPN)`