Location Privacy Protection in Distributed IoT Environments Based on Dynamic Sensor Node Clustering

Short Communication

Abstract

One of the most significant challenges in Internet of Things (IoT) environments is the protection of privacy. Failing to guarantee the privacy ofsensitive data collected andsharedover IoT infrastructures is a critical barrier that delays the wide penetration of IoT technologies in several user-centric application domains. Location information is the most common dynamic information monitored and lies among the most sensitive ones from a privacy perspective. This article introduces a novel mechanism that aims to protect the privacy of location information across Data Centric Sensor Networks (DCSNs) that monitor the location of mobile objects in IoT systems. The respective data dissemination protocols proposed enhance the security of DCSNs rendering them less vulnerable to intruders interested in obtaining the location information monitored. In this respect, a dynamic clustering algorithm is that clusters the DCSN nodes not only based on the network topology, but also considering the current location of the objects monitored. The proposed techniques do not focus on the prevention of attacks, but on enhancing the privacy of sensitive location information once IoT nodes have been compromised. They have been extensively assessed via series of experiments conducted over the IoT infrastructure of FIT IoT-LAB and the respective evaluation results indicate that the dynamic clustering algorithm proposed significantly outperforms existing solutions focusing on enhancing the privacy of location information in IoT.

Biography

Konstantinos Dimitriou he is from national technical university of athens in Greece

Note:- This work is partly presented at joint event on International Conference on Virology and Immunology (July 19-20, 2021 | Paris, France)