A Secure User Authentication and Key Agreement Scheme for HWSN Tailored for the Internet of Things Environment

Hamidreza Yazdanpanah[1], Mahdi Azizi and Seyed Morteza Pournaghi

Abstract: Internet of things (IoT) is the term used to describe a world in which the things interact with other things through internet connection or communication means, share the information together and or people and deliver a new class of capabilities, application and services; the world in which all things and heterogeneous devices are addressable and controllable. Wireless Sensor Networks (WSN) play an important role in such an environment since they include a wide application field. Researchers are already working on how to integrate WSN better into the IoT environment. One aspect of it is the security aspect of the integration. In 2014, Turkanovi´c proposed a lightweight user authentication and key agreement protocol for heterogeneous WSN(HWSN) based on the internet of things concept. In this scheme, a remote user can access a single desired sensor node from the WSN without the necessity of firstly connecting with a gateway node (GWN). Moreover, this scheme is lightweight because it based on simple symmetric cryptography and it uses simple hash and XOR computations. Turkanovi´c et al.'s scheme had some security shortages and it was susceptible to some security attacks. Recently Farash et al. proposed an efficient user authentication and key agreement scheme for HWSN tailored for the Internet of Things environment based on Turkanovi´c et al.'s scheme. Although their scheme is efficient, we found out that this scheme is vulnerable to some cryptographic attacks. In this paper, we demonstrate some security weaknesses of the Farash et al.'s scheme and then we propose an improved and secure mutual authentication and key agreement scheme.

Category / Keywords: cryptographic protocols / Wireless Sensor Networks; Internet of Things ; Mutual Authentication; Key Agreement

[1] **Contact author:** yazdanpanah.hr@gmail.com