Cellular automata based user authentication scheme using identity-bits commitment for wireless sensor network

ABSTRACT

In Wireless Sensor Network (WSN) communication, authentication between the communicating nodes is an important aspect and has gained intensive interest from the researcher all around the world. With the advance of the technology where the communication devices are all in small form factor, high speed and low cost authentication scheme for generating Message Authentication Code (MAC) is definitely a demand. This paper introduces a new fast and lightweight authentication scheme based on Cellular Automata (CA) utilizing a so called Identity-bits Commitment embedded in a temper resistance chip inside the wireless sensors. The security analysis shows that our scheme is secure against thwart replay attack and lightweight for fast implementation.

Keyword: Cellular automata; Authentication; Wireless sensor network