Jordan University of Science and Technology

RFID tags authentication by unique hash sequence detection

Authors: A. Alma'aitah, H. S. Hassanein and M. Ibnkahla

Abstract: With the rise of internet of things an immense number of RFID tags will be associated with different systems that require not only strong authentication protocols, but also time- and power- efficient protocols to authenticate more tags in a given time window. In current tag authentication protocols, a tag is considered authentic if the interrogators find a match to the tag's encrypted (e.g., using some hashing function) reply in the system's database. Tree-based authentication protocols provide rapid authentication by limiting the searched keys at the interrogator from O(N) to O(log(N)), where N is the number of leaves in the balanced tree. However, if one tag is compromised in such protocols, other tags will be at risk of being compromised. In this paper we propose Unique Hash Sequence Authentication (UHSA) protocol. The protocol utilizes tag-interrogator interaction, with a continuous wave (CW) sensor at the tag to cut off tags encrypted reply when the received bits are enough to determine next node in the tree without receiving the whole reply. Cutting off the encrypted reply limits the information that can be obtained by the adversary to compromise the tag. In addition, the reduction in tag reply length greatly enhances the time and power efficiency of the RFID system during the authentication process by more than 90% when compared to existing authentication protocols.