ABSTRACT

Radio frequency identification (RFID) system is the future of identification technology, RFID using radio waves to identify any object RFID tag is attached to; each tag has a unique identifier that distinguishes a tag from another.

RFID technology slightly replaces the barcode technology that is widely used nowadays, RFID technology offers more benefits than other identification systems, but its security drawbacks must be covered, the RFID system classification depends on the tag price or the resources required in operation.

This thesis focuses on ultra-lightweight authentication protocols, which use in low cost RFID tags, like the protocol proposed by Hung-Yu Chien. As he classifies the authentication protocol into four classes, the proposed protocol is of the fourth class, the ultra-lightweight protocol that proposed by Hung-Yu Chien provides strong authentication and strong integrity (SASI).

The following points describe the work that’s been done, and proposed the methodology and, calculate the performance of the proposed methodology:

1- The thesis analysis SASI protocol and the two attacks that were found by Hung-Yu Chien students that were found to break the synchronization of the protocol. It then was tested by implementing SASI protocol and applying the two attacks to prove they are able to de-synchronize the reader and the tag, and that was the outcome of the test. They lead to the de-synchronization between the reader and the tag .Though break SASI protocol.

2- Also this thesis is a proposed methodology for preventing vulnerabilities or attacks on SASI, and the implementation of this methodology is to prove the proposed concept, by applying the two attacks found by Hung-Yu Chien students and outcome that failed to break the proposed modification of the SASI protocols, after we apply the methodology to it, and these attacks failed to make the reader and the tag, out of synchronization. The reader and the tag communicate normally without any effect of these attacks.

As a conclusion of our proposed modifications:

- The modifications led to more secured RFID systems with a secured communication channel between the tag and the reader and between the reader and the backend database, which makes RFID systems counteract different de-synchronization attacks.

- The communication cost for SASI protocol is same as to the modified protocol, but the modification protocol is more secured than the unmodified SASI.

- There is a slight increasing in the storage overhead, however the storage increase still is in the accepted ranges, which is compatible with the standard storage capabilities of RFID Tags.

- The message exchange between the reader and the tag used in mutual authentication is still almost the same in modification and slightly increased in some proposed modification scenarios.