ABSTRACT

Radio Frequency Identification (RFID) technology is a powerful tool for identification of any object uniquely. Bar code or similar kind of technologies are also can be used for identification of the objects. However, the accuracy of object identification is far better in RFID technology since it does not have any line-of-sight constraint. The popularity of this technology has also been boosted due to its low cost. RFID technology becomes a cost effective solution by using small amount of hardware. Therefore, implementation of any application in this technology is a challenging task. This technology is one of the most pervasive computing technology and vulnerable to various kinds of attacks such as eavesdropping, replay attack, etc. However, we cannot use any standard cryptographic primitive in this technology in order to provide security against these attacks. Proper lightweight cryptography primitives need to be used without compromising the security.

Due to pervasive property of RFID technology, authentication is an important requirement in various RFID applications to restrict the non-legitimate access to certain resources. Many lightweight authentication schemes have been proposed till date. However, many authentication schemes suffer from location privacy problem, i.e., the objects can be tracked by using the information communicated during the authentication process. We propose a solution that can be applied over the existing authentication schemes that suffer from the location privacy problem and hence the tracking of objects can be avoided. However, this solution requires a small amount of additional hardware (288 gates) in RFID tag for its implementation.

We have also identified the vulnerability of de-synchronization attack in the authentication scheme proposed by Khor et al. (2010) and suggested a solution to fix this problem.

The detection probability of an object is low when it is attached with a single RFID tag. This can be improved by attaching multiple number of tags in a manner such that if any part of the object is within the coverage area of the reader, at least one tag attached to the object will be visible. The existing authentication schemes suffer from low

object detection probability since they assume that the objects are attached with single tag. Theses schemes cannot be extended to multi-tag environment, since they use one set of security related information for an object and keeping the same information in multiple tags attached to the same object is vulnerable. The adversary can easily compromise all the tags by compromising only a single tag. Therefore, an authentication scheme needs to be designed for multi-tag environment that can increase the difficulty for the adversary without compromising the detection probability of the object. In the present thesis, we propose two lightweight and secure authentication schemes in multi-tag environment. In the first authentication schemes, all the tags are allowed to respond on a request from an RFID reader. This increases traffic congestion in the communication medium between the object and the reader. In order to overcome this problem, we propose another authentication scheme. In this scheme, an object is attached with multiple number of active tags, one of which performs the authentication task. If this tag is not present within the coverage area of the reader, it obtains information through other tags attached to the same object. Hence, the detection probability of an object does not decrease. Though the proposed scheme uses multiple tags, the traffic congestion does not increase as a result of single response from each object.

Sometime, an object needs to be found from a large set. Any authentication scheme can be extended for this purpose. However, this approach is inefficient since the probability of useless computation due to the tags attached to the undesired objects is almost 50%. Similar to the existing authentication schemes for single tag environment, existing object searching schemes, which assume that the objects are attached with single tag cannot be extended to multi-tag environment. In the present thesis, we propose a secure and lightweight object searching scheme in multi-tag environment. The proposed scheme has been designed in such a way that the probability of computation due to the undesired tags is only 0.07%.

Some applications require the coexistence of a group of two or more relevant objects that can help to perform a particular event. Absence of one or more objects in the group can produce a wrong outcome. An assurance in the form of a proof of coexistence of the

desired objects can help to execute the event without any error. This problem can be solved using RFID technology. The existing proof generation schemes assume that the objects are attached with single tag and cannot be extended to multi-tag environment. In this thesis, we initially propose a secure and lightweight proof generation and validation scheme in multi-tag environment for a group of two objects. Later we extend the protocol to adopt a group of arbitrary number of objects.

In summary, the areas of contribution of this thesis are three-folds, (i) object authentication, (ii) object searching and (iii) coexistence proof generation and validation. This thesis proposes a solution to fix the tracking attack problem in the existing authentication schemes and then fix the de-synchronization problem in the authentication scheme proposed by proposed by Khor et al. (2010). It also proposes two authentication protocols, an object searching protocol and a coexistence proof generation protocol. The proposed protocols in this thesis are based on multi-tag RFID system and these protocols have been analyzed properly to evaluate the applicability.

Keywords: Multi-tag RFID, security, lightweight protocols, authentication, coexistence proof