Abstract

RFID uses radio frequency waves to track and identify objects. RFID system consists of tags and readers. Passive RFID tags are more popular now days due to its simpler circuitry, lower weight and lower cost. Generally passive tags are attached with an object for unique identification. A tag contains information about the particular product, to which it is attached. RFID reader is used to interrogate the tag to get the identity of the product attached with. RFID has numerous applications such as inventory management, asset tracking, library management etc. One of the major problems with RFID system is that whenever a reader interrogates a tag, all the tags residing in the read zone of the reader responds to the reader, which results in a collision at the reader's side. Thus makes it impossible to read the tags in time. To minimize the problem of collision at the reader side several anti collision algorithms has been proposed, but none of the algorithm concerns about the security aspect. Security is another major problem of RFID system. RFID tag discloses its identity to any reader which interrogates the tag, so any illegitimate reader can obtain the information contained in the tag. Now a day's situation is much worse because not only unique identification number but also user information such as name, address, phone number and other relevant information's of consumer are stored in the tag. There are different manufacturers of tags who provide tags with 1kb memory, which is large enough to store such kind of consumer information without
pointing to backend database. In such cases security concern is much more as eavesdropping may lead to disclose some personal data, which is a big threat for consumer. Implementing cryptographic algorithm is not a feasible solution for the RFID system, as this may result in complex circuitry, and which in turn may raise size and cost of the passive tags. Here in this paper we have combined both the problem of collision and security together to find a suitable solution which solves both the problems. Taking into consideration of simpler circuitry and lower price of passive tags, here we propose a solution which modifies existing anti collision protocol to make it secure so that any illegitimate reader cannot read the information contained in the tag thus protecting tags from malicious reading.

**References**

- Benetton undecided on use of &apos;smart tags&apos;. Associated Press, 8 April 2003.

**Index Terms**
Keywords
Secure anti collision protocol  Secure Tree based algorithm