работы. Поскольку радиопередачи считывателя отличимы от шума на расстоянии вплоть до нескольких десятков метров, злоумышленник может без проблем накопить секретную информацию (в данном случае – список номеров) о метках, установив подслушивающее устройство на безопасном удалении от считывателя. Во избежание подобной ситуации, в существующий алгоритм следует внести коррекции.

Такой модифицированный алгоритм назван *защищённой антиколлизией.*

Во-первых, считыватель будет вещать некоторый бит номера метки лишь в том случае, если последний бит был принят с коллизией, таким образом, выделяя для дальнейшей работы одну из конфликтующих подгрупп; в остальных случаях он будет подавать меткам некоторую общую команду «передать следующий бит номера». Во-вторых, для каждой новой сессии получения номеров меток, последними будут генерироваться случайные двоичные вектора (R - в данном случае длиной 16 бит), передаваемые побитно в эфир непосредственно перед вектором уникального 96-битного номера (ID): R|ID, где | - конкатенация векторов. При этом к моменту, когда в процессе антиколлизии очередь дойдёт до передачи самого номера одной из меток, с большой вероятностью (P= 1-(N-1)/2^16, где N – число меток в поле) из всех меток не приостановленной останется только одна и считыватель не «раскроет» ни одного бита её номера.

Система считыватель-метка, использующая данный алгоритм, реализуется в виде модели поведенческого описания аппаратуры (язык Verilog). Основными элементами модели являются блоки считывателя и метки. Данные устройства работают по принципу конечных автоматов, состоят из основных «подблоков»: тактирования, инициализации и синхронизации; преобразования входных данных, формирования передающей последовательности; случайного генератора; «подблока» управления.

Приведённая модель представляет собой новый, более защищённый, при учёте жёстких ограничений по ресурсам радио-меток, вариант описания системы радио-идентификации, позволяет виртуально тестировать данную систему, и при некоторой доработке может быть реализована в готовых устройствах.

SAFE ANTICOLLISION IN INDUSTRIAL RADIO FREQUENCY IDENTIFICATION(RFID) SYSTEMS AS A HARDWARE DESCRIPTION MODEL

Laykov Y.M.
OOO «Rider»,
Moskva

In order for a reader to be able to gather data from all tags in it's field, a particular procedure must be implemented in the RFID system's algorithms. The procedure is called "anticollision" and is designated to solve errors caused by simultaneous response of several tags to a reader's request. These errors are named "collisions" – events that occur when a reader is unable to recognize the data received due to it's overlapping. The existing anticollision algorithms are based on:

a) allocating tags' responses to so called "time slots" when every tag is assigned to some fixed time interval where it replies to reader's requests;

b) mask usage – a bit sequence of length up to the size of identification number (ID) – in order to address a subgroup of tags sharing some common prefix;

c) bit-by-bit selecting of tags which is similar to (b), except for subgroup addressing type that is bit-by-bit here.

The last case is the most appropriate because it provides the highest operation speed.

This anticollision algorithm is called "binary tree walking algorithm". It assumes that a reader alternately broadcasts every single bit of IDs of each tag in it's range. As a response to each incoming bit from a reader, every tag that contains this bit in it's ID will simultaneously send back the next bit. On the other hand those tags that didn't find the bit received to be equal to the corresponding one will switch to some suspended state until the reader applies command to resume in normal mode. As a result of longer range of reader's transmissions (up to several dozens of meters), an adversary can easily collect private data (in this case – a list of IDs) from tags by installing an eavesdropping device at safe distance from a reader. To avoid this the existing algorithm has to undergo few modifications.

Such modified algorithm shell be named "safe anticollision".

First of all a reader will broadcast a bit of tag's ID only if the last bit is received with collision. Thus one of the conflicting subsets of tags will be selected for further interaction. When no collision is detected, the reader shell broadcast some constant command "send next ID bit". Secondly in the beginning of new anticollision session, the tags in the field generate some random binary vectors R(in this case 16 bit length) that are sent bit-by-bit immediately before IDs: R|ID, where | - represents vectors concatenation. Therefore when it's turn for a tag's ID itself to be sent, there is high probability(P=1-(N-1)/2^16, N – number of tags in the field) that this tag will be the only unseived one. As a result the reader will broadcast no bits of the tag's ID.

RFID system consists of two main types of devices: reader and tags. The suggested algorithm is implemented in the system's hardware description language model (Verilog). The model is made of reader and tag blocks, which function as cellular automata. The blocks are separated into main "subblocks": clock, initialization, synchronization, input data converter, output stream converter, random number generator and control "subblock".

The proposed model is a new, more secured description of digital part of RFID system hardware. It is designed with consideration of harsh resource constraints of tags due to cost limits. With help of the model it is possible to virtually test this system and synthesize a logical scheme.