Robotics & Automation Engineering Journal
ISSN: 2577-2899

Juniper Publishers
key to the Researchers

Research Article
Volume 5 Issue 2 - January 2020
DOI: 10.19080/RAEJ.2020.05.555656

Robot Autom Eng J

Edge Data Security in Industrial Iot for RFID-Based Robots

Javed Gaggatur S[1]*, Javeria A[2] and Prabhakar M[2]

[1]*Computer Science and Engineering, Reva University, Bangalore, India*

[2]*King Consultants - Education, Bangalore, India*

Submission: October 18, 2019; **Published:** January 16, 2020

***Corresponding author:** Javed Gaggatur S, King Consultants - Education, Bangalore, India

Abstract

RFID has become the preferred technology for monitoring in industrial internet of things applications like supply chain, medical industry, vehicle tracking and warehouse monitoring. The data security threats seen in the IIoT applications are denial of service (DOS) attacks. A proposal for edge data security in industrial IoT for RFID-based robots was presented. An RFID-Sensor based backscatter communication system was used as an example and the methods of RFID encoding to secure the data was proposed as a solution for edge data security. The data encoding scheme works well in the multi-tag single-reader environment. The proposed solution appears to present a low-cost solution for edge data security in Industry 4.0.

Introduction

Radio frequency identification (RFID) technology has applications over a wide range of domains in industrial internet of things (IIoT) including supply chain industry, medical industry, vehicle tracking, warehouse monitoring. The rapid acceptance of RFID technology is significantly due to its simple architecture, low power operation, spontaneous multiple sensing and non-line-of-sight detection. The data on the RFID tag contains information about the ID tag, the source and destination of the product contents of the tagged product, if any. Industrial warehouses use RFID tags to track the product movement from entry to shipment. The RFID data contains sensitive information about the source and destination, which the tag reader placed on the robot is processed and the product is sorted and placed in the warehouse. The RFID data can be encrypted/ unencrypted depending on the application and the nature of the product being handled. Information leakage in an RFID system can be minimized, however cannot be eliminated Figure 1.

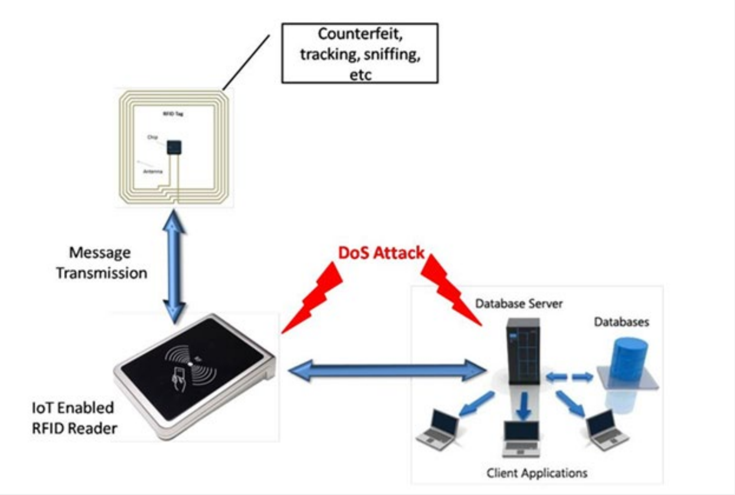


Figure 1: Security threats in RFID based systems.

A security protocol is proposed that aims at a cross layer security mechanism that makes the system immune to side channel attacks. A side-channel attack is any attack based on information gained from the implementation of a computing system. Timing, power, sound and electromagnetic leaks provide additional information, which may be exploited [1]. The side channel attacks addressed here are Simple Power Analysis (SPA) and Differential Power Analysis (DPA) attacks. The SPA and DPA attacks occur with relative ease over the wireless channel during a validated communication, between the reader and the server, with a high probability of a Denial of Service (DOS) attack. An attempt to block the message being sent from a valid tag to a valid reader followed by the server results in a DOS attack. The protocol proposes a distributed RFID system, wherein data processing does not depend on a centralized server for validating every tag reader operation. The proposed system uses ultra-high frequency (UHF) passive/active tags, whose read range can reach about 9m. UHF passive tags have a decent non-line-of-sight communication, store about 100KB of data and operate at 860-960MHz. The rest of the paper is organized as follows: Section II discusses the RFID tags and its encoding. Section III describes the system architecture and section IV discusses the proposed security protocol in IoT Architecture.

Radio Frequency Identification (RFID) Tags

Ultra-high frequency (UHF) RFID Tags

The RFID reader emits radio waves of specific frequencies through RFID antennas in a wide range of emission as shown in Figure 2. The waves" give energy" to the tags so that they can communicate by emitting a unique ID. The reader processes the data so that we can integrate them into our application and give them meaning. The typical reading range is 0-12 meters. Gen2 Ultra high frequency (UHF) RFID systems consist of readers, antennas, printers, and RFID tags or tags [2].

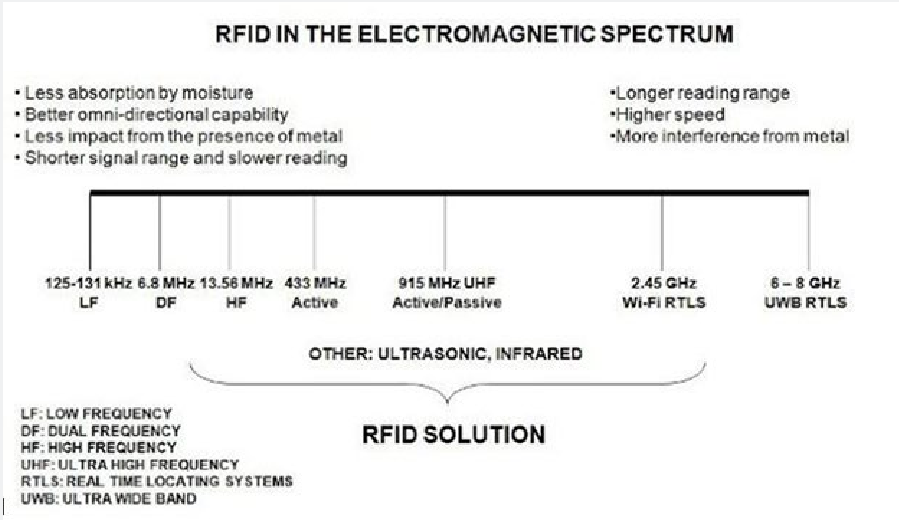

RFID IN THE ELECTROMAGNETIC SPECTRUM
• Less absorption by moisture
• Better omni-directional capability
• Less impact from the presence of metal
• Shorter signal range and slower reading
•Longer reading range
•Higher speed
•More interference from metal
125-131 kHz LF
6.8 MHz DF
13.56 MHz HF
433 MHz Active
915 MHz UHF Active/Passive
2.45 GHz Wi-Fi RTLS
6 – 8 GHz UWB RTLS
OTHER: ULTRASONIC, INFRARED
RFID SOLUTION
LF: LOW FREQUENCY
DF: DUAL FREQUENCY
HF: HIGH FREQUENCY
UHF: ULTRA HIGH FREQUENCY
RTLS: REAL TIME LOCATING SYSTEMS
UWB: ULTRA WIDE BAND

Figure 2: RFID in the electromagnetic spectrum [2].

Types of memory in RFID tags

Generation 2 radio frequency identification (RFID) tags are comprised of an antenna and an integrated circuit (IC) [3]. The ICs for Gen 2 tags contain four types of memory:

a. Reserved memory

b. Electronic Product Code (EPC) memory

c. Transponder ID (TID) memory

d. User memory

The TID memory is used only to store the unique tag ID number by the manufacturer when the IC is manufactured. Typically, this memory portion cannot be changed. If the user needs more memory than the EPC section has available, certain ICs have extended user memory which can store more information. When it comes to user memory, there is no standard in how many bits of memory are writable on each tag. Typically, the extended memory is no more than 512 bits, but there are some high memory tags with up to 4K or 8K bytes of memory. This is the second writable memory bank for Gen 2 ICs [3].

RFID-Based Application System Architecture

RFID-Sensor Backscatter Communication System

The RFID-Sensor backscatter communication system architecture in Figure 3a is adapted for the proposed security application [4,5]. The communication system comprises of an RF energy harvestor circuit containing a RF-DC and DC-DC converters. The energy harvestor DC output powers the Oscillator and Buffer.

When the DC power is available, oscillator oscillates with the period T. Buffer output is given to a spike generator which is a passive circuit completely. The spike generator produces spikes on every rising edge of the oscillator signal. Thus, we have one spike for every T seconds. Output of spike generator is given to a band pass filter.

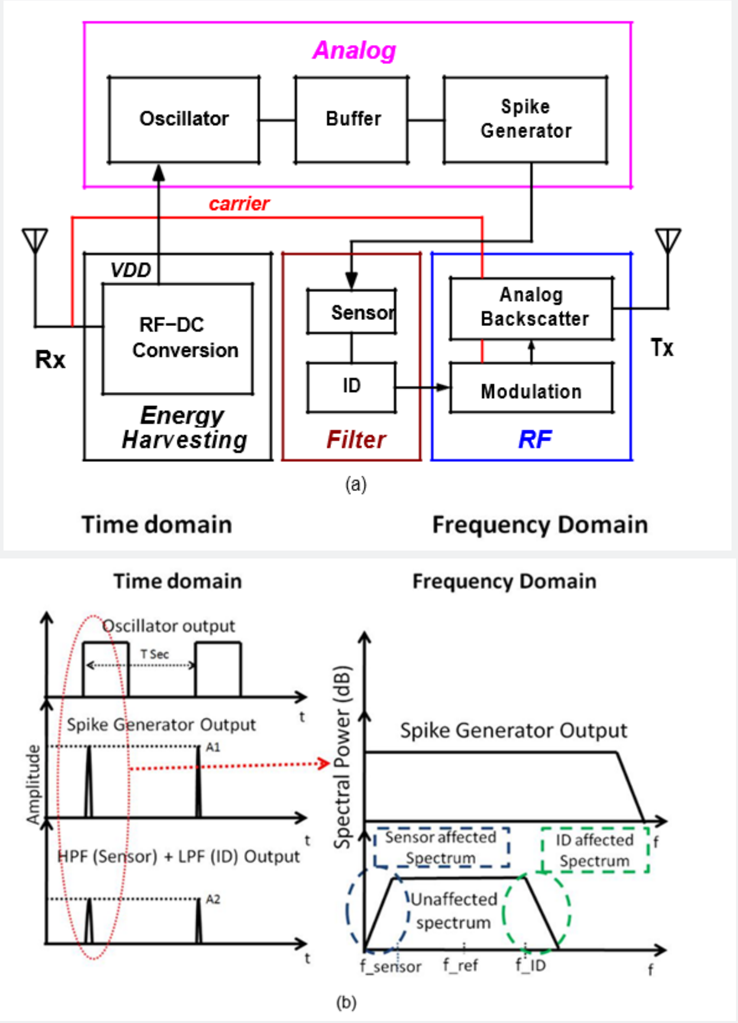


Figure 3: (a) Block Diagram of the proposed spike-based RFID communication system (b) Operation of system in time and frequency domain, showing the spike modulation by sensor and ID [4]..

Operation

The principle of operation is based on three simple concepts and the tag shall combine all the three before the data transmission.

a) When we compress a time domain signal, it leads to signal expansion in frequency domain.

b) Low Pass Filter output can be attenuated depending on the values of R and C.

c) Electrical sensors output value is governed by the value of R or C.

The operating principle of the system is as shown in Figure 3b. Firstly, a narrow spike is generated by spike generator circuit which can provide enough bandwidth. Secondly, the spike is passed through the low pass filter (LPF) and a high pass filter (HPF), which are passive circuits controlling the sensors and ID information. The operating sequence is summarized in the flowchart in Figure 4. The ID and Sensor in Figure 3a behave as finite delay cells having a time signature. Figure 5 shows the timing signal containing the time signature of the ID and sensor, which drives the transmitter [5]. The transmitter output in Figure 6 has the time signature of the ID and Sensor along with the carrier signal from the reader.

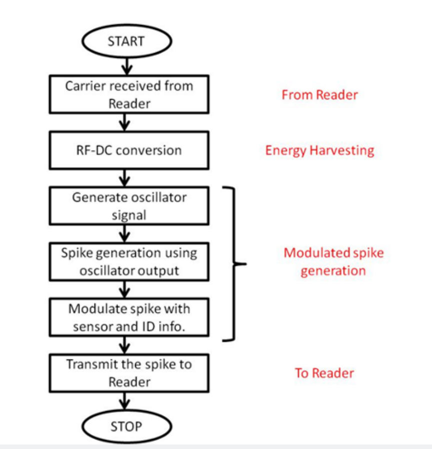

START
Carrier received from Reader
From Reader
RF-DC conversion
Energy Harvesting
Generate oscillator signal
Spike generation using oscillator output
Modulate spike with sensor and ID info.
Modulated spike generation
Transmit the spike to Reader
To Reader
STOP

Figure 4: Flowchart describing RFID-based Application system operation [4].

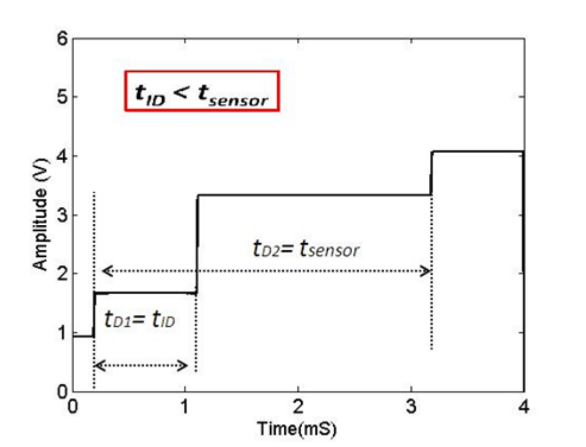


Figure 5: Timing signal generation for the tID and tsensor transmission [5].

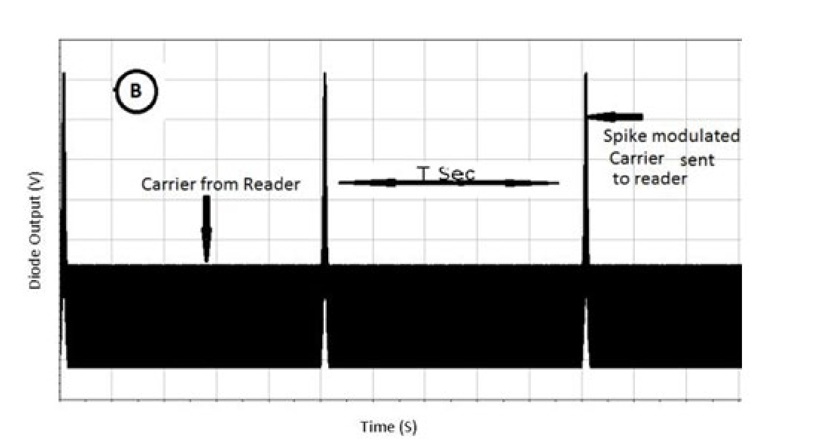


Figure 6: Transmitter output with the ID and Sensor information of the spike [4].

How to cite this article: Javed Gaggatur S, Javeria A, Prabhakar M. Edge Data Security in Industrial Iot for RFID-Based Robots. Robot Autom Eng J. 2020; 5(1): 555656. DOI: 10.19080/RAEJ.2020.05.555656

Multi-Tag Environment

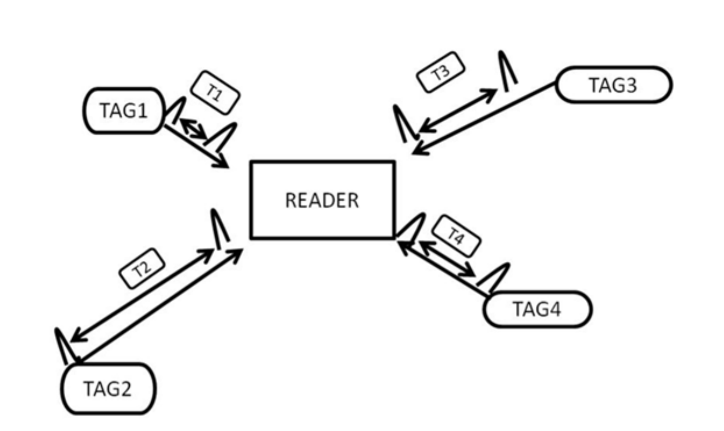


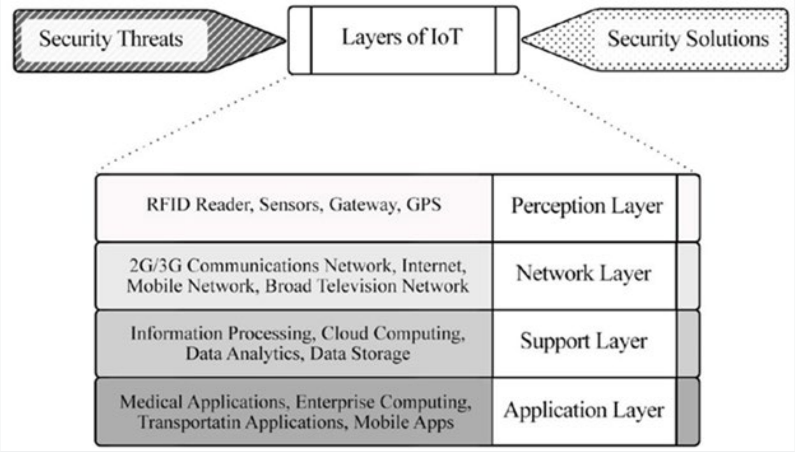
Figure 7: A system environment showing the need for multi-tag IDs and method to avoid multi-collision tag read and write [4].

The application of object monitoring in a warehouse [6] using RFID includes working with multiple objects and tags, and each tag presenting a unique ID. Figure 7 shows a typical multi-tag environment with different time signatures for the ID's at the tag reader. The tag collision is mitigated with the varying time signatures of each tag. The information present in the timed signal can be interfered using a different voltage causing a DOS attack.

The proposed security protocol adds an additional encoding to the tag information. This encoding protects the information from the DOS attacks by recovering the information successfully in the tag reader.

Security in IOT Architecture

Figure 8 gives the proposed IoT architecture needed for the implementation of the proposed application stack.



RFID Reader, Sensors, Gateway, GPS	Perception Layer
2G/3G Communications Network, Internet, Mobile Network, Broad Television Network	Network Layer
Information Processing, Cloud Computing, Data Analytics, Data Storage	Support Layer
Medical Applications, Enterprise Computing, Transportatin Applications, Mobile Apps	Application Layer

Figure 8: Security needed for the IoT Architecture.

Perception Layer: The sensor technology, intelligence embedded technology, nano technology and tagging technology are in this layer. Main purpose of the layer is the identification of unique objects and the collection of information from the physical world with the help of its sensors.

Network Layer: It contains WSN, optical fiber communication networks, broad television networks, 2G/3G communications networks, fixed telephone networks and closed IP data networks for each carrier. Transfer of collected information from sensors, devices, etc., to an information processing system is under the responsibility of this layer.

Support Layer: The layer involves information processing systems which takes information in one form and processes (transforms) it into another form. This processed data is stored in a database and will be available when there is a demand. This layer works very closely with applications and hence, fits well in the application layer.

Application Layer: In this layer, there are practical and useful applications which are developed based on user requirements or industry specifications such as smart traffic, precise agriculture, smart home, mining monitor, etc.

Security of perception layer

The security requirement for the internet of things (IoT) architecture is broadly defined in Fig. 8. IoT devices machines and equipment's such as RFID readers, sensors, gateways, GPS and other devices require to be secured efficiently. OWASP has identified poor physical security in the top 10 IoT vulnerabilities. The first step is to ensure that only authorized people can have access to sensitive data produced by physical objects, that why a physical identity and access management policy need to be defined. Authentication and authorization requirements from IoT are satisfied in this similar fashion. Data collection is an important issue for this layer. This issue can be examined in two separate headings. In one heading which is presented as multimedia data collection, there are some recommended security techniques such as multimedia compression, stenography, water marking, encryption, time session and intellectual property. The second heading is image data collection, to use security in images as image compression, and CRC. Cryptographic processing is one of the main tasks in security mechanisms for sensor data on IoT. These operations that are often used in order to guarantee privacy of data include encryption and decryption, key and hash generation, and sign and verify hashes.

Encoding RFID

The UHF Active RFID tags contain an integrated circuit or chip (Figure 1), which can be encoded and be printed with a bar-code or number. The tags can also be encoded with USB readers, fixed readers or portable readers. The EPC or TID is read in the tag, whose coding is composed of a unique number that comes from the factory. The EPC space of the tag is what is recorded, modified and with which we normally interact. The tags have an internal memory (User memory) where we can save additional information [2].

a. **EPC Re-encoding:** The Electronic Product Code (EPC) number can be re-encoded with unique information. For example, in inventory applications the item's or product's unique serial number can be encoded. Another example would be in race timing applications where marathon runner's bib number can be encoded as the EPC number.

b. **Scheme specific EPC generation:** A scheme of data generation is proposed for logistics and warehousing applications. The EPC data string can have a varying bit length for the various segments like Header, Filter value, Item reference, partion and serial number. The schemes can be modified based on the companies or geographical locations.

Conclusion

RFID has become the preferred technology for monitoring in industrial internet of things applications like supply chain, medical industry, vehicle tracking and warehouse monitoring. The data security threats seen in the IIoT applications are denial of service (DOS) attacks. A proposal for edge data security in industrial IoT for RFID-based robots was presented. An RFID-Sensor based backscatter communication system was used as an example and the methods of RFID encoding to secure the data was proposed as a solution for edge data security. The data encoding scheme works well in the multi-tag single-reader environment. The proposed solution appears to present a low-cost solution for edge data security in Industry 4.0.

References

1. (2009) Inc Wikipedia Side-Channel Attack. https://en.wikipedia.org/wiki/Side-channel attack.
2. https://www.dipolerfid.com/en/blog/How-UHF-RFID-System-Works.
3. Shain Armstrong (2013) Types of Memory in RFID Tags. https://blog.atlasrfidstore.com/types-of-memory-in-gen-2-uhf-rfid-tags.
4. Machnoor M, Gaggatur JS, Sanjeev K (2015) Novel spike-based architecture for RFID and Sensor communication system. In IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society p. 003714–003719.
5. Gaggatur JS, Machnoor M (2015) Solar-powered spike-based communication system with analog back scatter. in 2015 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (Prime Asia) p. 127-132.
6. Javed Gaggatur S, Gaurab Banerjee (2019) Time of arrival measurement for indoor distance monitoring in 130-nm CMOS. Measurement 146: 372-379.

How to cite this article: Javed Gaggatur S, Javeria A, Prabhakar M. Edge Data Security in Industrial Iot for RFID-Based Robots. Robot Autom Eng J. 2020; 5(1): 555656. DOI: 10.19080/RAEJ.2020.05.555656

DOI: 10.19080/RAEJ.2020.05.555656

How to cite this article: Javed Gaggatur S, Javeria A, Prabhakar M. Edge Data Security in Industrial Iot for RFID-Based Robots. Robot Autom Eng J. 2020; 5(1): 555656. DOI: 10.19080/RAEJ.2020.05.555656