RFID AUTHENTICATION

Zulkharnain Muhammad

Department of Electrical, CAIT.,
Jazan University
Jazan, Saudi Arabia
zbadruzzama@jazanu.edu.sa

Abstract

Smart UHF RFID devices are the most secure ones as on now. They work on 860 to 960 Mhz. They can hardly be hacked or reverse engineered, because of the secure technology involved in it. It is almost not possible to clone it, neither can it be attacked. It uses no cryptography. It can thus be used for smart tag for security application. It permits only legitimate user to have access. First, he needs to enroll, using the tag. Here it is ensured that the possession of the device exists with the right owner along with machine and deep learning methods. Thus, it is verified in these two ways. This is useful for adoption in smartwatches. The acceptance is almost ninety seven percent. Deep learning related false acceptance is less than one percent. The latency is found to be less than two seconds, which is almost the time in feeding passcode.

.

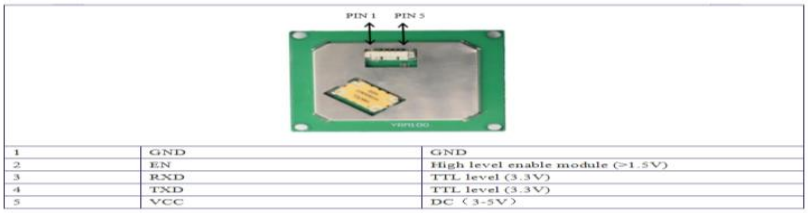
Keywords: Smart RFID, Smart UHF device, Smartwatch authentication.

1. Introduction

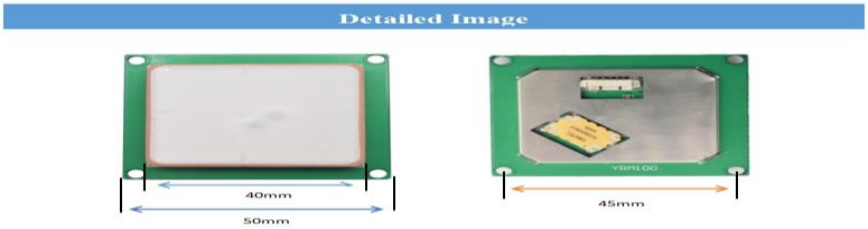
RFID is Radio frequency Identification. It is a cheap access control technique, in range of 12 m. It uses a reader and server for back end. It also uses Tags. every tag is concerned to a particular user only. The reader sends radio signals allocated to a particular user. It enquires about a particular tag. It has an assigned transmission range. When the concerned tag if present in the close vicinity allocated for it, it responds. It gives the authentication information. This is what is termed as electronic product code. It is also the cryptographic message. Then the reader forwards this information to the server. The server finally verifies it. Then the access to the concerned is given. This can be used for authentication of say a room, a computer or a parking slot. Nowadays passive ultra-high frequency RFID, is mostly used. The reader uses the modulation technique of radio frequency signals. Passive tags are those which do not use battery. They backscatter the signals. The reader uses antenna system to transmit. The tag also uses antenna, which sends the received signal to an integrated circuit inside it. Energy in this signal helps modulation along with data inside it. This communication is thus by electromagnetic waves. The received signal is decoded by reader.

2. APPLICATION

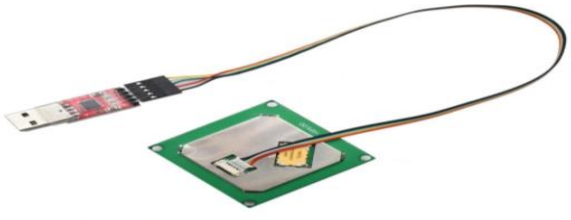
This secure system is useful in hospitals. The availability of say a nurse in the hospital in a certain area can be checked by this system. Logistics companies can also use this system. It is also used with physically impaired ones. Similarly tracking a person in a given location can also be done using this. As cryptography is not supported here it has limited applications, if there is need of high security. It can also be used in competitions like using the tag as the ankle band for swimming triathlon, to note the timings. Following is the module of the system used almost in all of the above applications given:



1	GND	GND
2	EN	High level enable module (>1.5V)
3	RXD	TTL level (3.3V)
4	TXD	TTL level (3.3V)
5	VCC	DC (3-5V)



YRM100 UHF RFID Integrated reader module



YRM100 UHF RFID module connect with cable

3. Latest developments

If more security is desired in this application, the system costs almost 20 times more than the normal ones without cryptography. Such tags are already manufactured by the company NXP. RFID signals can be used to recognize human gestures. This is called gesture-based authentication. It is the promising field for future car control system. It can be used for instance by the driver to change the volume of sound system. Microsoft Kinect also uses this technique to control the dashboard for the games used in it. Ford is using this technique to open the door or tailgate by waving ankles. This is useful when the driver's hand is occupied with carrying heavy load. UHF RFID Tags are being used in apparel markets.

4. Proposal

Here in this paper is discussed the method of using a smart device using authentication of RFID system, with tags. First the device needs to be enrolled into the system. Then the RFID system verifies twice. Fist the tag code, and next the nearness of the device and tag. If both are valid the authentication is successful. The user has to carry the smart device with him. This is a fast and invulnerable. The man in the middle attack is also made impossible in the system.

The coexistence of Tag and device can be verified using correlation of inertial accelerometer data and the RFID backscattering. The tag needs to be shaken and tapped multiple times for 3 seconds, in vicinity of the smart device connected. This move should be detected by the accelerometer. The signals should have change in phase. The server detects the phase and acceleration information. If the correlation is a strong one the authentication is given

5. Problem in implementation:

If the genuine user due to some other reasons waves his device, then a hacker nearby doing sync movement similarly, can benefit in hacking. This is called sync-attack. Anyhow this attack can be prevented by the genuine user by using sequence of taps. A novel machine learning algorithms have to be used to recognize the taps and shakes.

Even though the acceleration and phase information can't be directly compared, they can be extracted twice. Support vector machine method can also be used, for more security.

6. Literature Review:

Today's ubiquitous computing demands constant update in security measures to counter the challenges posed by the hackers around. RFID is the base for further development of such ubiquitous computing. The ever-increasing exploitable channels for adversaries have been creating more challenges. Thus, many researchers have opted to generate more publications on RFID security in almost every security journal related to that [7,8,9,10,11].

7. Conclusion:

The latest type of RFID tags is not able to execute conventional cryptography. Hence new less computationally complex security algorithms need to be developed, so that the cost of RFID tag doesn't increase without compromise in the concerned security system. The analytical

process [12], has been worth mentioning in security enhancement, experimenting based on that can help improve the RF communication. This way object recognition becomes easy without complex methodology being involved, without privacy violation and forgery. The Proposal [13] of ultralight weight authentication protocol of RFID system based on MDS code is also highly appreciable. Thus, by implementing all these protocols RFID system authentication can be made more secure than that existing as on now.

8. Acknowledgements:

The author Zulkharnain, thanks CAIT, Jazan university, Saudi Arabia, for providing research facilities for experimenting on RFID technology.

9. References

1. Fall Detection Using Commodity Smart Watch and Smart Phone

Artificial Intelligence Applications and Innovations, 2014, Volume 436SBN : 978-3-662-44653-9 Ilias Maglogiannis, Charalampos Ioannou, George Spyroglou, Panayiotis Tsanakas

2. The Influence of Menu Structure and Layout on Usability of Smartwatches Fan Mo and Jia Zhou

Journal: International Journal of Mobile Human Computer Interaction, 2018, Volume 10, Number 1, Page 1

DOI: 10.4018/IJMHCI.2018010101

3. J Gesture-based incident reporting through smart watches

Panagiotis Kasnesis, Christos Chatzigeorgiou, Lazaros Toumanidis and Charalampos Z. Patrikakis

Conference: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Year: 2019, Page 249

DOI: 10.1109/PERCOMW.2019.8730586

4. Gesture-based incident reporting through smart watches

Pa nagiotis Kasnesis, Christos Chatzigeorgiou, Lazaros Toumanidis and Charalampos Z. Patrikakis

Conference: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Year: 2019, Page 249

DOI: 10.1109/PERCOMW.2019.8730586

5. Online Fall Detection Using Recurrent Neural Networks on Smart Wearable Devices

Mirto Musci, Daniele De Martini, Nicola Blago, Tullio Facchinetti and Marco Piastra

Journal: IEEE Transactions on Emerging Topics in Computing, 2021, Volume 9, Number 3, Page 1276

DOI: 10.1109/TETC.2020.3027454

6. Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pages 103–111, New York, NY, USA, 2003. ACM Press.

7. Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols. In Advances in Cryptology – CRYPTO'05, volume 3126 of LNCS, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.

8. Ari Juels and Stephen Weis. Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137, 2006. [23] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard. In SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pages 47–58, Washington, DC, USA, 2005. IEEE Computer Society

9. Tri van Le, Mike Burmester, and Breno de Medeiros. Forward-secure RFID authentication and key exchange. Cryptology ePrint Archive, Report 2007/051, 2007.

10. M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch. From identification to authentication - a review of RFID product authentication techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

11. T. Li and R. Deng. Vulnerability analysis of EMAP - an efficient RFID mutual authentication protocol. In Second International Conference on Availability, Reliability and Security – AReS 2007, Vienna, Austria, April 2007.

12. Cho, Jung-Sik & Kim, Soo-Cheol & Yeo, Sang-Soo. (2011). RFID System Security Analysis, Response Strategies and Research Directions. 371 - 376. 10.1109/ISPAW.2011.76.

13. P. K. Maurya, H. Ghosh and S. Bagchi, "MDS code based ultralightweight authentication protocol for RFID system," in IEEE Access, doi: 10.1109/ACCESS.2023.3239530.