International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST523102108

Study of Security Threats, Authentication Protocols and RFID Networks

Ankesh Kumar[1], Dr. K. B. Singh[2], Dr. Pankaj Kumar[2]
[1]Research Scholar, University Department of Physics, B. R. A. Bihar University, Muzaffarpur, Bihar, India
[2]P. G. Department of Physics, L. S. College, Muzaffarpur, B. R. A. Bihar University, Muzaffarpur, Bihar, India

ARTICLEINFO

Article History:
Accepted: 10 April 2023
Published: 29 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
876-879

ABSTRACT

In this paper, we studied about security threats, authentication protocols and RFID networks. Wireless sensor networks (WSN) and radio frequency identification (RFID) are two important wireless technologies that have a wide variety of applications and provide limitless future potentials. RFID facilitates detection and identification of objects that are not easily detectable or distinguishable by using current sensor technologies.

Keywords: RFID, WSN, Radio Waves, Sensor.

I. INTRODUCTION

Integration of RFID with WSN is one of the techniques employed for enhancing more applications and security. Three types of integrations are suggested. The first one is heterogeneous network architecture with a mix of RFID tags and WSN nodes and a smart station that will be used for collecting information from two networks. The second type of integration includes integration of the reader and a WSN node in one device. The third type is a smart active tag that merges functionality of a WSN node and an active tag. The possible ways of integrating WSNs into the existing RFID network based on the standards defined by EPCGlobal.

Integrity is a concept that ensures that data can only be modified, replaced by authorized agents. Integrity deals with both the correctness and reliability of data. Integrity requires that the data being sent is complete, unmodified and entirely in its original form. OSP aims to provide confidentiality, authentication and integrity of messages by employing the security primitives. Some of them are used much more in industry and academia then others. In addition, WSN nodes can be independent or attached to objects/people. It is mandatory for secure network to follow the following goals. Adherence to these security goals should present a network with threat deterrence properties. Energy transfer is the way by which passive RF devices are powered. The energy transfer mechanisms are inductive coupling, capacitive coupling, and passive backscattering.

Memory can be classified into read-only, write-once and read-write.

Optimized Security Protocol (OSP) provides comprehensive security by guaranteeing confidentiality, authentication and integrity of messages, so that WSNs are protected against the threats that they are exposed to. By combining the properties of RFID (identifying and positioning) and WSNs (sensing, identifying and positioning) we can define different application scenarios for combining RFID and WSNs.

II. MATERIALS AND METHOD

RADIO FREQUENCY IDENTIFICATION

Radio frequency identification (RFID) uses electromagnetic field of radio frequency for automatic identification of objects with a unique ID number which is stored in the attached tag [1]. Both RFID and barcode systems have the same goal; identifying objects without human intervention.

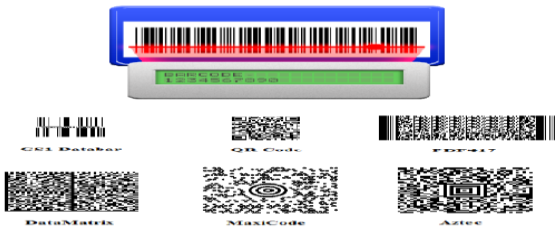

Figure 1: Barcode Examples[5]

WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) consist of sensing, computing, and communication elements and are used for monitoring environment's temperature, humidity, pressure, etc. In other words, WSN is a network which is made up by nodes that sense and control the environment cooperatively. Nowadays, WSN is used in many areas such as traffic control, health care monitoring, healthcare applications, and supply chain.

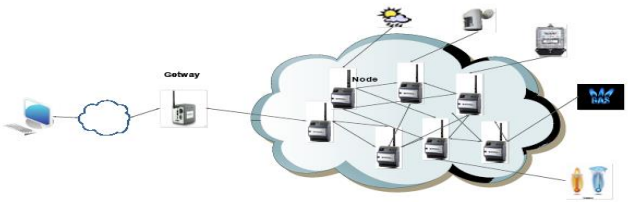

Figure 3: Components of Wireless Sensor Network

III.RESULTS AND DISCUSSION

It is needed to maintain products in certain conditions sensed by the smart nodes which are strongly related to temperature and gas. In case of any unpredictable situations such as gas release, the alarm must be alerted. The temperature of the environment can be monitored continuously and be set if required. It is noteworthy that smart nodes detect products types in order to store them in the particular places when they negatively affect one another. WSN and RFID can work in the same ISM frequency without any collision. It also can be used in separate frequencies because they have different modulation techniques.

Table 1: Description of transitions

T1 through 2	Transitions of parts to the conveyors
T3 through 9	Transitions of parts on the conveyors
T10 through 11	Transitions of AGV 1 and 2 to load parts respectively
T12 through 15	Transitions of AGVs to own locations in room 1
T16 through 17	Transitions of AGVs 1 and 2 in room 2
T18 through 19	Transitions of AGVs 3 and 4 in room 2
T20 through 23	Transitions of ASRS robots
T24	Transition of parts to the vehicle
T25	Transition of vehicle
T26 through 30	Transferring orders to related applications software

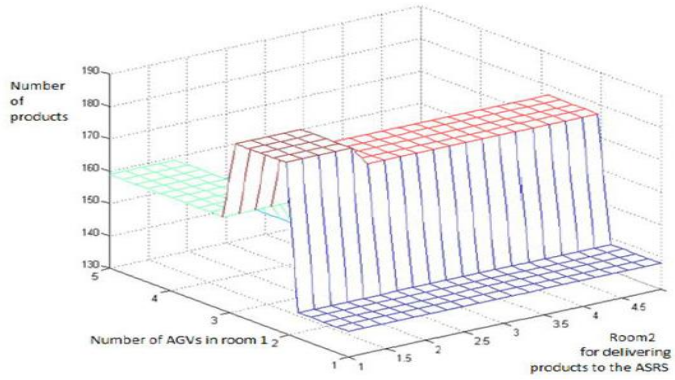

Figure 1: Optimization Model for determining AGVs

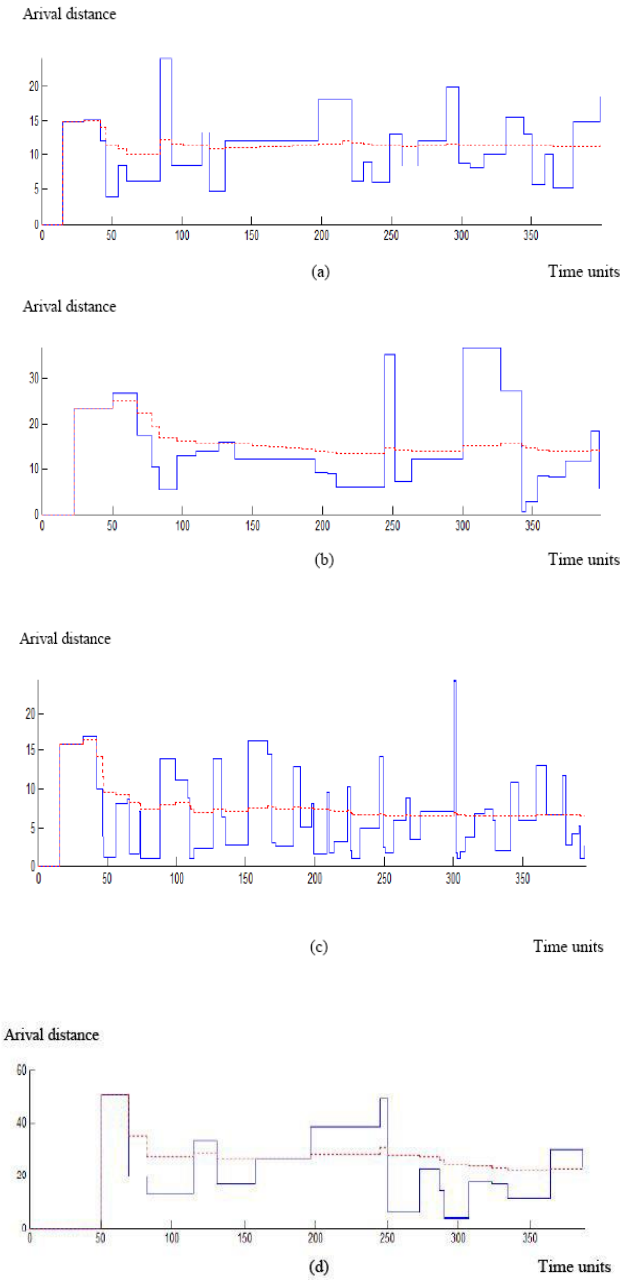

Figure 2: Arrival distance commads

Figure 2 depicts the total number of products which have been entered and delivered during 395 time units in the supply chain system. As can be seen, two rooms are provided that totally 194 products come to the first room and 186 products exited and rest of them stayed in the room. Therefore, 183 products were brought to the next room by related AGVs and also 170 products delivered to the retail. In this case, there are two types of the products which the first type is shown by blue color and the second type is shown by pink color.

Table 2: Performance evaluation of the system

	Throughput Sum	Throughput Rate	Throughput Dist.	Utilization
Input parts	194	0.49181	2.0333	-
AGV 1	29	0.073518	13.6022	0.78572
AGV 2	33	0.083658	11.9534	0.8209
AGV 3	61	0.15464	6.4666	0.1552
AGV 4	17	0.043097	23.2037	0.096318
ASRS	170	0.43097	2.3204	0.70127
Output parts	180	0.45798	2.1835	-

IV. CONCLUSIONS

In high-end applications, it is possible to integrate RFID tags with wireless sensor nodes and wireless devices, such that the integrated tags are able to communicate with many wireless devices which are not limited to readers. The main difference between the tags with integrated sensors are traditional RFID tags which communicate only with readers, while the tags in this class are able to communicate with other wireless devices, including tags themselves. Therefore, the tags in this class are able to communicate with each other and form a multiple hop network.

V. REFERENCES

[1]. S. W. Wang, W. H. Chen, C. S. Ong, L. Liu and Y.W. Chuang, RFID application in hospitals: A case study on a demonstration RFID project in a taiwan hospital, system sciences, HICSS'06, Proceedings of the 39th Annual Hawaii International Conference 8 (2006).

[2]. R. Das, RFID forecasts, players & opportunities 2007–2017, Enterprise Networks & Servers, (March 2007).

[3]. C.F. Hernández, P.H. Ibargüengoytia-González, J.G. Hernández, J.A. Díaz, "Wireless Sensor Networks and Applications: a Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, Pages 264 -273. March 2007.

[4]. Hasan Tahir, Syed Asim Ali Shah, "Wireless Sensor Networks– A Security Perspective", 12th IEEE International Multitopic Conference, Karachi, pp. 189-193, December 23-24, 2008.

[5]. Yee Wei Law, Paul J.M. Havinga, "How to secure a wireless sensor network", Published in Intelligent Sensors, Sensor Networks andInformation Processing 2005. IEEE pp 89-95.

[6]. L. Zhang and Z. Wang, Integration of RFID into wireless sensor networks: Architectures, opportunities and challenging problems. Proceedings of the 5th International Conference on Grid and Cooperative Computing Workshops (GCCW'06) (2006).

[7]. Yu, S.-C. (2008). Implementation of an innovative RFID application in libraries. Library Hi Tech, 26(3), 398–410. Retrieved from http://doi.org/10.1108/07378830810903328

[8]. Zhang, D., & Shi, X. (2011). Self-service management platform design for library based on RFID. In 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings (pp. 7237–7240.) Retrieved from http://doi.org/10.1109/AIMSEC.2011.6010604

[9]. RFID On Line Access 22-03-2013 Http://Www.Rfid4u.Com/Downloads/Library%20Automation%20Using%20 RFID.Pdf

[10]. Hamdoun, S.; Rachedi, A.; Benslimane, A. RSSI-based localization algorithms using spatial diversity in wireless sensor networks. Int. J. Ad Hoc Ubiquitous Comput. 2015, 19, 157–167.

[11]. Zhu, A.; Fan, T.; Gu, Z.; Lv, Q.; Li, C.; Ran, L. Indoor localization based on a single-tone SIMO-structured Doppler radar system. In Proceedings of the 2018 IEEE Radio and Wireless Symposium (RWS), Anaheim, CA, USA, 15–18 January 2018.

[12]. Hatem, E.; Colin, E.; Abou-Chakra, S.; El-Hassan, B.; Laheurte, J.-M. Constellations of active UHF-RFID tags for indoor positioning. In Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN), Nantes, France, 24–27 September 2018; pp. 1–4.

[13]. Ela Innovation, SA. (2014) Ela Innovation active RFID tag and reader manufacturer. Available online: http://www.rfid-ela.eu/ (accessed on 20 July 2015).

[14]. Hatem, E.; Colin, E.; Abou-Chakra, S.; El-Hassan, B.; Laheurte, J.-M. 3D Modeling for Propagation of UHF-RFID Tags' Signals in an Indoor Environment. In Proceedings of the 2nd IEEE Middle East and North Africa Communications Conference (MENACOMM), Manama, Bahrain, 19–21 November 2019; pp. 1–6.

[15]. Hoppe, R.; Wölfle, G.; Jakobus, U. Wave propagation and radio network planning software WinProp added to the electromagnetic solver package FEKO. In Proceedings of the International Applied Computational Electromagnetics Society Symposium, Firenze, Italy, 26–30 March 2017; pp. 1–2.

Cite this article as :

Ankesh Kumar, Dr. K. B. Singh, Dr. Pankaj Kumar, "Study of Security Threats, Authentication Protocols and RFID Networks ", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 876-879, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRST523102108
Journal URL : https://ijsrst.com/IJSRST523102108