RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES BENEFITS AND APPLICATION IN INDUSTRY

[1]Gautam Kumar Nag, [2]Dr.Jaya Prakash Sinha
Research Scholar, SSSUTMS,
Research Guide, SSSUTMS

Abstract: Radio Frequency Identification (RFID) is an automatic identification method based on the remote storage and retrieval of data through the use of RFID tags or transponders. The technology requires an RFID reader and RFID tag and uses AIDC technology. AIDCrefers to methods for automatically identifying objects, collecting data about them, and entering that data directly into computer systems (ie, without human intervention). AIDC is the process or means to obtain external data, especially through the analysis of images, sounds or videos. This article will provide the technology behind Radio Frequency Identification systems, identify Radio Frequency Identification applications in different industries, and discuss the methodologicalissues of implementing Radio Frequency Identification and the strategies to address those challenges. Radio Frequency Identification business processes, including reverse logistics and supply chain, decision making within and between organizations, because of their ability to provide highly accurate and automated real-time information.

Keywords: Radio Frequency, RFID technology, Industry, Security

Introduction

To capture data, a transducer is employed which converts the actual image or a sound into a digital file. The file is then stored and at a later time it can be analyzed by a computer, or compared with other files in a database to verify identity or to provide authorization to enter a secured system. The technology requires some extent of cooperation of an RFID reader and an RFID tag. An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions. The second is an antenna for receiving and transmitting the signal. There are generally two types of RFID tags: active RFID tags, which contain a battery, and passive RFID tags, which have no battery.The origins of RFID technology can be traced way back to laboratory research in the 1940s that focused on reflected power communication. Its commercial use began in the 1980s, primarily in railroad and trucking industries (30). These applications used battery powered active RFID tags and proprietary systems to track and manage capital assets, such as rail cars and cargo containers. The expansion of RFID into a wide variety of business applications has been due to the reduction in the cost of RFID technology through the use of non-battery powered passive tags that can replace bar codes as a means of gathering information.

Related work

It should be noted that since RFID is in its infancy, the research on RFID is fragmented and limited. We briefly review the available RFID literature. For example, Jones et al. (1) discussed the opportunities and implementation challenges of RFID for retailers in the United Kingdom (UK). Småros and Holmström (2) considered RFID as a data capture method in consumers' refrigerators to develop a new type of e-grocery related service. Brewer and Sloan(3) regarded RFID as an intelligent tracking technology in manufacturing to support logistics planning and execution. Jansen and Krabs considered RFID to control returnable containers. Kärkkäinen discussed the potential of RFID implementation for increasing supply chain efficiency of short shelf life products through an RFID trial conducted at UK retailer Sainsbury's. Lapidesuggested the benefits of RFID for forecasting, such as improved forecast accuracy, more accurate point of sale data from retailers, and better tracking of products sold with or without promotion. Moreover, Kärkkäinen and Holmströmconsidered RFID as a wireless product identification technology to enable material handling efficiency, customization and information sharing in a supply chain. McFarlane and Sheffiused a ship/receive (S/R) pair structure to examine four basic logistics processes (shipping, transportation, receiving and in-facility operations) and discussed how low cost RFID can be used to improve each process. Hosakasimulated hospital bedside and nursing station conditions to automatically authenticate the matching of patients and their medical articles in order to reduce medical errors, while Janz et al.presented the technological and behavioral challenges encountered during the implementation of an RFID patient tracking system at the Elvis Presley Memorial Trauma Unit in Memphis, Tennessee.

Application of RFID

This section discusses the application of RFID technology in retailers and manufacturers, which are currently the major adopters of RFID technology.Radio Frequency Identification (RFID) Solutionscan play a detrimental role in industrial applications, increasing their automation and accuracy. The applications of RFID in health care and other fields are also discussed.

Automotive Industry:

Perhaps, one of the most common RFID applications in automotive industry is vehicle immobilizer. A vehicle immobilizer is basically a system that prevents a vehicle from being driven if a wrong RFID tag is provided. Almost over 40 percent of new cars produced in North America are equipped with some sort of RFID-enable immobilizer. Besides this antitheft system, RFID technology is also applied to the inventory management in automotive industry to maintain inventory status.

Payment Transactions

In the United States, many RFID-based payment system can be found in marketplaces such as Speedpass offered by ExxonMobil and ExpressPay conducted by American Express. In addition, RFID-based payment systems can also be found in transportation areas around the world such as SmarTrip used in Washington D.C. Metro system, EasyCard for Taipei Metro in Taiwan, Nagasaki Smart Card system in Japan, Oyster Card for London Transportation, and so on. Perhaps, the most remarkable RFID-based payment system in the world is the Octopus system in Hong Kong. The Octopus system allows users to use just a single smart card to pay for not just transportation fares but almost everything around users.

Retailing:

RFID-based applications in retailing are mainly for product tracking and inventory management. In June 2003, Wal-Mart Corporation issued a mandates for its top 100 suppliers to adopt passive RFID tag to all the shipments sent to three of its Texas distribution centers by January 2005. One month after the deadline, the CIO of Wal-Mart stated that more than 5 million tag reads had been taken. Also, the read rate at the case level has passed 90 percent for cases on carts, but the read rate at the case level were very low (averaging in 66 percent) for cases on pallets. Adopting RFID technology has benefited Wal-Mart in a 16 percent reduction in out-of-stock items. Moreover, replenishment for out-of-stock items is three times faster than using bar code system, and stores equipped with RFID are more effective at replenish out-of-stock items. Overall, an estimation shown by Research firm Sanford C. Bernstein & Co. stated that annually over $8 billion could be saved once Wal-Mart has fully deployed RFID through all its locations.

Security and Privacy Threats

In a taxonomy model of RFID security threats is presented. This model has two levels. There are three layers in the first level, threats of application layer, threats of communication layer, and threats of physical layer. In the second level, types of system-specific attacksassociated with each layer are presented there. The taxonomy mode of security threats is shown in Fig.1.

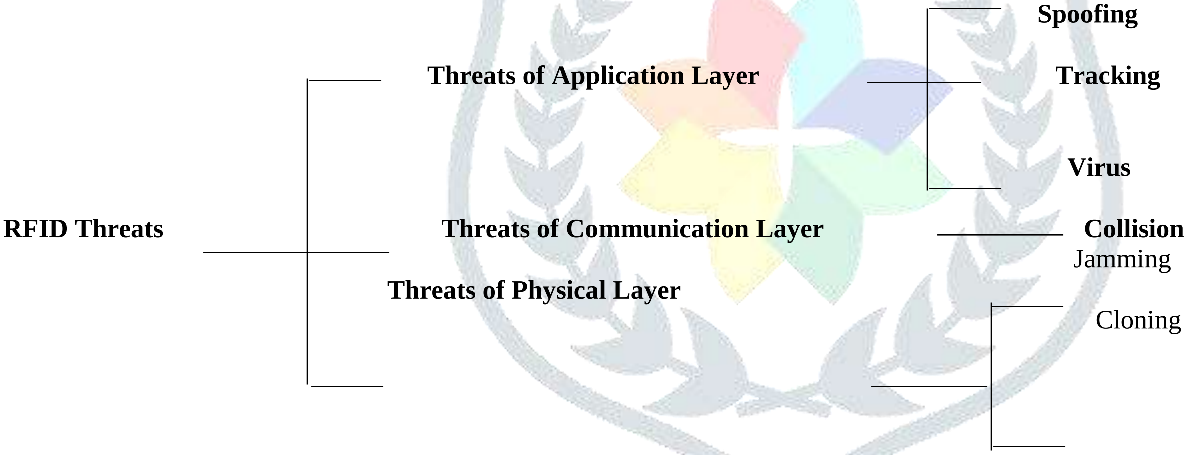
Spoofing
Threats of Application Layer
Tracking
Virus
RFID Threats
Threats of Communication Layer
Collision
Jamming
Threats of Physical Layer
Cloning

Figure 1- Taxonomy Model of RFID Security Threats(Ding Zhen-hua, et al.,)

Physical Layer:

Type of attacks in physical layer included RF eavesdropping, jamming and cloning, generally violate electromagnetic properties (RF signal) in the physical layer. Due to the reason that RFID tags and readers communicate wirelessly, RF eavesdropping can be achieved by simply using an antenna to listen to the communication. RF eavesdropping can also lead to Spoofing, Replay, and Tracking attacks if an adversary can figure out the encoding method. Jamming attack can be accomplished by constantly broadcasting RF signals. Doing so, any nearby RFID readers' operations will be disrupted. Therefore, avoiding RF signals from RFID readers reach tagged items. Cloning can be attained by reverse engineering the tags or by building a device that mimic the tag's signal.

Communication Layer:

Collision is the main threat in communication layer which violates the way the RFID reader single out a particular tag for communication. When more than one tag responds to RFID reader's query, collision takes place. An attacker can send out one or more signals at the same time to respond RFID reader's query in order to create collision. When collision happens, the communication between RFID tags and readers stalls. Therefore, a collision attack is also a type of Denial of Service attack (DOS).

Application Layer:

Spoofing, Replay, Tracking, Desynchronization, and Virus are associated to application layer. They basically violate the properties of applications such as the identification of tag, the operation related to backend system, and personal privacy (in [14], privacy threat is considered a type of security threat). Spoofing attack can be achieved by forging a tag to act as a valid tag. Doing so, an attacker can use the forged tag to fool the RFID reader and backend system to gain products and services. Replay attack focus on consuming the computing resource of the whole system. Tracking attack is related to user's personal privacy. For example, a user with a tagged item which might be read by an attacker'sreader if the reader is compatible with that tag. This will lead to several privacy issues such as location disclosure, purchase history, and so on. Desynchronization attack is a threat of desynchronizing the ID between backend system and tag's ID. This can make the tag useless. Desynchronization attack occurs when the RFID reader is failed to write ID to tags or when backend system can not transmit ID to RFID reader. Virus attack can be accomplished by injecting virus into the tag and then use SQL injection to attack the backend system.

Confidentiality:

In a general RFID system, confidentiality of data can be breached by an attacker through the five elements described above. Gaining data through tag, RFID reader, and backend system, an attacker needs to have physical access. In gaining data through links, close proximity is required for an attacker to listen to the communication. Example of attacks to breach confidentiality through link (RF link) between tag and RFID reader are tracking/tracing, sniffing, and spoofing. Tracking and tracing attacks can use the sniffed ID to track a person. This also implies privacy issues. In addition, sniffed ID can be used to clone tags. Spoofing attack can be accomplished by replay and relay attacks.

Conclusion

Radiofrequency identification technology should focus on a different perception of closed system applications. The technology has aroused much enthusiasm for their practical cost-benefit considerations. The co-existing protocol, communication and data levels within the International Organization for Standardization (ISO) ensure the worldwide growth of radio frequency identification technology. Despite the challenges of research and innovation, radio frequency identification technology will reach the highest level in the food production industry. Above all, the security of man consumes to show a healthy society. The research of radio frequency identification will introduce it into various applications.

References

[1] AbhishekMajumder, NityanandaSarma "DEMAC: A Cluster-Based Topology Control for Ad Hoc networks" International Journal of Computer Science Issues, vol.7, no.5, pp.82-88, 2010.

[2] Aditya Karnik and Anurag Kumar, "Distributed Optimal Self-Organization in Ad Hoc Radio", IEEE/ACM Transactions on Networking, vol. 15, no.5, pp. 1035-1045, 2007.

[3] Akerberg, J., Gidlund, M., &Bjorkman, M. (2011, July). Future research challenges in wireless sensor and actuator networks targeting industrial automation. In Industrial Informatics (INDIN), 2011 9th IEEE International Conference on (pp. 410-415). IEEE.

[4] Akyildiz, I. F., &Vuran, M. C. (2010). Radio (Vol. 4). John Wiley & Sons.

[5] Alemdar, H., &Ersoy, C. (2010). Radio for healthcare: A survey. Computer Networks, 54(15), 2688-2710.

[6] AlineCarneiroViana, Marcelo Dias de Amorim, Serge Fdida, Jose Ferreira de Rezende, "Self-Organization in Spontaneous Networks: The Approach of DHT-Based Routing Protocols", Journal of Ad Hoc Networks, vol.3, pp.589-606, 2005.

[7] Alzoubi .K, Wan P-.J, and Frieder .O, "Message-Optimal Connected Dominating Set Construction for Routing in Mobile Ad Hoc networks", 3rd ACM International Symposium on Mobile Ad Hoc networking and Computing (MobiHoc '02), pp.157-164, 2002.

[8] AmitabhaGhosha, Sajal K. Dasb, "Coverage and connectivity issues in radio: a survey", Pervasive and Mobile Computing, vol.4, pp.303-334, 2008.

[9] Anastasi, G., Conti, M., & Di Francesco, M. (2011). A comprehensive analysis of the MAC unreliability problem in IEEE 802.15. 4 radio. Industrial Informatics, IEEE Transactions on, 7(1), 52-65.

[10] AnandSrinivas, Gil Zussman, and EytanModiano, "Mobile Backbone Networks Construction and Maintenance", MobiHoc'06, pp.166-177, 2006.

[11] Anindya Iqbal, Nafees Ahmed , Mostofa Akbar "Directional Antenna Based Connected Dominating Set Construction for Energy Efficient Broadcasting in Wireless Ad Hoc network", International Conference on Computer and Electrical Engineering, pp.839- 843, 2008.

[12] Baccour, N., Koubaa, A., Mottola, L., Zuniga, M. A., Youssef, H., Boano, C. A., &Alves, M. (2012). Radio link quality estimation in radio: a survey. *ACM Transactions on Sensor Networks (TOSN)*, *8*(4), 34.

[13] Baccour, N., Koubaa, A., Mottola, L., Zuniga, M. A., Youssef, H., Boano, C. A., &Alves, M. (2012). Radio link quality estimation in radio: a survey. *ACM Transactions on Sensor Networks (TOSN)*, *8*(4), 34.

[14] Baccour, N., Koubaa, A., Mottola, L., Zuniga, M. A., Youssef, H., Boano, C. A., &Alves, M. (2012). Radio link quality estimation in radio: a survey. *ACM Transactions on Sensor Networks (TOSN)*, *8*(4), 34.

[15] Bachir, A., Dohler, M., Watteyne, T., & Leung, K. K. (2010). MAC essentials for radio. *Communications Surveys & Tutorials, IEEE*, *12*(2), 222-248.

[16] Bang Jensen J, Gutin G, Yeo A, "When the Greedy Algorithm Fails", Discrete Optimization, vol.1, pp.121-127, 2004.

[17] Bao L, Garcia-Luns .J Aceves, "Topology Management in Ad Hoc networks", Proceedings of ACM MobiHoc '03, pp.129-140, 2003.

[18] B.Narmadha, M.Ramkumar, K.Vengatesan, M.Srinivasan, "Household Safety based on IOT", International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939, Volume.5, Issue 4, pp.1485-1492, December 2017.