Neil B Dahlqvist

Advisor: Emmanuel Tentzeris

Team name: Raising the Steaks

Data storage in RFID systems

Introduction

Automatic identification of a variety of objects, from grocery items to livestock, is crucial in any business or industry. The well-known barcode labels triggered a revolution in identification systems. They are widely use and inexspensive but inadequate in many cases. Perhaps, the major limitation is the need for line of sight access of the coded data. The ideal solution is contactless transfer of information between the data carrying device and its reader. The use of radio waves and silicon chips made this approach feasible and the procedure is called Radio frequency identification (RFID). The big idea that drives the RFID is the commercial vision to change the way any demand-supply chain operates. In the future, RFID enabled stores, warehouses and refrigerators will monitor the consumption in real time and will signal the inventory when it needs more stuff. One of the biggest advantage of the RFID technology over optical barcodes is the comparatively large data storage capacity. Therefore, it is imperative to look with more detail into the challenges of databases implementation and data storage in RFID systems.

Data Storage Capacity

Barcodes usually have a very limited data storage capacity. Conventional 1-dimesional barcodes can store just few bytes of data. The EAN13-code used in Europe stores 13 numerical digits identifying country, product manufacturer, and product type. It is not possible to identify each item uniquely and to hold all the relevant information describing the item like price, ingredients, or best before date [1]. The same problem exists in other numbering system schemes like the Universal Product Code (UPC) and the International Standard Book Number (ISBN code). More complex 2-dimensional barcodes or larger 1-dimensional barcodes extend the amount of data that can be stored. However, this comes at the cost of a larger printing area. RFID transponders offer a more comprehensive data storage capacity. They can serve as a means of unique identification for different kinds of objects like documents, food, or animals. More complex transponders can store an even larger amount of data. For example, data describing the tagged objects, a documentation of the object's history or even data putting the object in the context of other objects [2].

Databases

The best approach to cope with the storage limitations is to store all required data in databases. In the case of optical barcodes, the data is taken as an index to the object's data in the database. Since the database resides on a server and the data is stored on hard disks, there are few limitations upon the data that can be stored there. There are basically two possible data storage locations in a product identification system: directly on a barcode/transponder or within a backend database [3]. As the storage capacity of barcodes is so limited, one can only store an identifier and has to keep all other relevant data in a database. In RFID systems, one can store data either directly on the transponder, in a backend database, or even redundant at both locations. RFID databases associate tag-identifying data with arbitrary records.

These records may contain product information, tracking logs, sales data, or expiration dates. The storage location affect quality characteristics of the overall system differently. Such characteristics are costs, speed, flexibility, and security in the resulting system [4].

System Flexibility

In the business world, companies have to adjust to new situations quickly. Therefore, flexibility is a key factor for a company's success on the market. Flexible RFID techniques with respect to data storage are the ones that store only identifiers on the transponders and as much product data as possible in the backend. One of the advantage of storing identifiers on the transponder and of keeping all other data in backend databases is the system's compatibility with existing barcode systems. A second advantage is transponder reuse and cooperation between different companies within the supply chain [5].

System Security and Privacy

The connection between the reading device and the transponder is wireless, using the air as the transmission medium. Thus communication is public and transmitted data can easily be intercepted. It is possible to apply cryptographic protocols to secure the transmission, but this requires the use of RFID transponders that have more functionality than just data storage and that are thus more expensive [6]. Storing unencrypted data on transponders exposes it to public attacks. As long as the transponders remain within controlled and closed areas such as factory building, this threat can be neglected. Because data stored on the transponder can be eavesdropped during communication, it is reasonable to store as much data in the backend as possible. An effective and flexible access control can be implemented there and data does not have to be transmitted over insecure communication channels. From a data security perspective, when leaving the factory, the transponder should only contain the information that is needed by other companies that process these transponders. This is the only way to avoid possible threats posed by industrial espionage and to respect the principle of data security to store no more than the absolute required data [6].

Conclusion

Falling prices for transponders and increasing reliability in RFID technology have resulted in the favorable usage of RFID systems in today's industries. Service provides and enterprises will consider the application of RFID devices in areas where the technology is now too expensive or unreliable. The use of databases as the primary method of data storage will make companies focus their attention in ways to improve secured RFID systems and enhance privacy.

References

[1] Diekmann, T., Melski, A., & Schumann, M (2013). "Data-on-network vs. Data-on-tag: Managing data in complex RFID enviroments". *Proceeding of the 40th Annual Hawaii International Conference on System Sciences, Hawaii,* 224-233

[2] Ward, M., Kraneneburg, R., & Backhouse, G. (2011). "RFID: Frequency, standards, adoption and innovation", *JISC Technology and standards Watch,* 1-36. Retrieved from http://www.rfidconsultation.eu/docs/ficheiros/TSW0602.pdf

[3] Hass, L. M., & Miller, R. J (2011). "Transforming heterogeneous data with database middleware: Beyond integration". *Bulletin of the IEEE Computer Society Technical Committee on Data engineering,* 1-6

[4] Landt, J. (2014). "The history of RFID". *Potentials IEEE*, 24(4), 8 – 11.

[5] Lin, D., Elmongui, H. G., Bertino, E., &Ooi, B. C. (2011). "Data management in RFID applications". *DEXA*, 434-444

[6] Juels, A. (2014). RFID Security and Privacy. A Research Survey. *Selected Areas of Cryptography*. To appear, 2011