Yan Qiao, Shigang Chen, Tao Li

RFID as an Infrastructure

– Monograph –

August 28, 2012

Springer

Chapter 1
Introduction

Abstract RFID (radio frequency identification) tags are becoming ubiquitously available in object tracking, access control, and toll payment. The current application model treats tags simply as ID carriers and deals with each tag *individually* for the purpose of identifying the object that the tag is attached to. The uniqueness of this book is to change the traditional *individual view* to a *collective view* that treats universally-deployed tags as a new infrastructure, a new wireless platform on which novel applications can be developed. This chapter argues for such a paradigm shift. It introduces the problems of tag estimation and information collection from RFID systems, and explains the challenges, laying the background for the rest of the book.

Key words: RFID, Radio-Frequency IDentification

1.1 What is RFID?

RFID (radio-frequency identification) is *the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking* [37]. The basic technologies for RFID have been around for a long time. Its root can be traced back to an espionage device designed in 1945 by Leon Theremin of the Soviet Union, which retransmitted incident radio waves modulated with audio information. After decades of development, RFID systems have gain more and more attention from both the research community and the industry.

A typical RFID system consists of one or multiple readers and numerous tags. Each tag carries a unique identifier (ID). Depending on the source of power, tags can be divided into three categories. 1) Passive tags are most widely used today. They are cheap, but do not have internal power sources. They rely on radio waves emitted from the reader for power, and have small operational ranges of a few meters. 2) Semi-passive tags contain internal batteries to power their circuits and allow longer reading distance. However, they still rely on a reader to supply its power for transmitting. 3) Active tags use their own battery power to receive and transmit information to readers. They have a much longer read range – 300 feet(91 meters) or more.

Consider a large warehouse in a distribution center of a major retailer, where hundreds of thousands of tagged commercial products are stored. In such an indoor environment, if we use passive tags, hundreds of RFID readers may have to be installed in order to access tags in the whole area, which is not only costly but also causes interference when nearby readers communicate with their tags simultaneously. It is not a good solution neither to use a mobile reader and walk through the whole area whenever we need information from tags. If the goal is to fully automate the warehouse management in a large scale, we believe battery-powered active tags are a better choice. Their much longer operational distance allows a reader to access numerous tags in a large area at one or a few fixed locations. Meanwhile, with richer on-tag resources, active tags are likely to gain more popularity in the future, particularly when their prices drop over time as manufactural technologies are improved and markets are expanded.

1.2 Why are RFID Technologies Important?

The barcode system brought a revolutionary change in the retail industry. Information can be embedded in the barcode. In particular, a product ID can be encoded. Once a reader retrieves the ID, it can use the ID to search a database to find all information about the product, which may include price, features, or even manufacture and shipping history. However, barcodes can only be read in close ranges with direct sight. This is fine when used for checkout in a retail store, but it is not suitable for warehouse management.

RFID technologies remove this limitation by integrating simple communication/storage/computation capacities in attachable tags, whose IDs can be read wirelessly over a distance, even when obstacles exist between tags and the RFID reader. The longer operational range makes them popular in automatic transportation payments, object tracking, and supply chain management[15, 26, 33]. Starting from August 1, 2010, Wal-Mart has begun to embed RFID tags in clothing[38]. If successful, these tags will be rolled out onto other product lines at Wal-Marts more than 3,750 U.S. stores[4]. That is one step towards cashier-less checkout, where a customer pushes his/her shopping cart to pass an RFID reader at the checkout, where information in the embedded tags is automatically read and a receipt is printed out.

1.3 What to be Expected Next?

In recent years, a relatively small number of research groups have been investigating novel ways in which future RFID systems can be used to solve practical problems.

Of course, RFID tags may be embedded in library books, passports, driver licenses, car plates, medical products, etc. In the current application model, tags are treated as ID carriers and they are dealt with individually for the purpose of identifying the object that each tag is attached to. Now, if we make a paradigm shift from this *individual view* to a *collective view*, an array of new applications and interesting research problems will emerge. Consider a major distribution center of a large retailer, assuming it applies RFID tags to all its merchandise. These tags, which are pervasively deployed in the center, should not be treated just as ID carriers for individual objects. Collectively, they constitute a new *infrastructure*, which can be exploited for center-wide applications. If we take one step further, we can make this infrastructure more valuable by augmenting tags with miniaturized sensors, such that they report not only static ID information but also dynamic real-time information about their environment or conditions of the tags themselves. If we take another step to consider security or tag mobility, more applications and research problems open up.

1.4 Tag Estimation

Imagine a large warehouse storing thousands of refrigerators, tens of thousands of furniture pieces, or hundreds of thousands of footwear. A national retail survey showed that administration error, vendor fraud and employee theft caused about 20 billion dollars lost a year [12]. Hence, it is desirable to have a quick way of counting the number of items in the warehouse or in each section of the warehouse. To timely detect theft or management errors, such counting may be performed frequently.

If each item is attached with a RFID tag, the counting problem can be solved by a RFID reader that receives the IDs transmitted (or backscattered) from the tags [35]. However, reading the actual IDs of the tags can be time-consuming because so many of them have to be delivered in the same low-rate channel and collisions caused by simultaneous transmissions by different tags make the matter worse. Naturally, we want to design a protocol for tag estimation that minimizes the execution time.

Is time efficiency the only performance metric for the RFID estimation problem? We argue that energy cost is also an important issue that must be carefully dealt with when active tags are used to cover a large area. Active tags are powered by batteries. A longer reading range can be achieved by transmitting at higher power. Recharging batteries for tens of thousands of tags is a laborious operation, considering that the tagged products may stack up, making tags not easily accessible. To prolong the tags' lifetime and reduce the frequency of battery recharge, all functions that involve large-scale transmission by many tags should be made energy-efficient.

1.5 Sensor-augmented RFID Systems

The deployment of RFID tags will not only make the objects in a warehouse wirelessly identifiable, but also provide an "infrastructure" that we can leverage to do other things. Consider a RFID system with miniaturized sensors incorporated into tags circuit [24, 26, 29], enabling them to collect useful information in real time. Such system is called *sensor-augmented RFID system*. A sensor may be designed to monitor the state of the tag itself, for instance, the residual energy of the battery. In this case, the information reported to the reader can be a floating-point number reflecting the percentage of remaining energy, or simply a single bit indicating whether or not the battery needs replacement. In another example, consider a large chilled food storage facility, where each food item is attached with an RFID tag that carries a thermal sensor. An RFID reader may periodically collect temperature readings from tags to check whether any area is too hot (or too cold), which may cause food spoil (or energy waste)[1].

A sensor-augmented RFID system imposes challenges that are fundamentally different from traditional sensor networks. For example, information collection is not difficult in a classical wireless sensor network [6, 7], where each sensor implements routing/scheduling/MAC protocols. If the MAC protocol is CSMA/CA, the sensors will be able to sense the channel and transmit their information when it is idle. In addition, they are able to detect collision and use random backoff to resolve it. However, in a sensor-augmented RFID system, the simplicity of RFID tags places many constraints on the solution space, often making an otherwise easy problem difficult to solve. For example, what if the hardware of tags does not support such an MAC protocol, let alone routing/scheduling protocols? What if their simple antenna cannot sense weak signal from peers for collision avoidance, let alone performing random backoff? Hence, the challenge is to do the same work of information collection with less hardware support.

1.6 Brief Overview of State-of-the-Art

Much existing work is on designing ID-collection protocols, which read IDs from all tags in an RFID system. They mainly fall into two categories. One is *ALOHA-based* [5, 16, 30, 31, 34, 42], and the other is *tree-based* [1, 2, 25, 44]. The ALOHA-based protocols work as follows: The reader broadcasts a query request. With a certain probability, each tag chooses a time slot in the current frame to transmit its ID. If there is a collision and the reader does not acknowledge positively, the tag will continue participating in the next frame. This process repeats until all tag IDs are read successfully. Zhang et al. [41] improve the ALOHA-based protocols by extracting useful information from collision slots through analog network coding.

---

[1] If a tag reports an abnormal temperature, the reader may instruct the tag to keep transmitting beacons, which guide a mobile signal detector to locate the tag.

The tree-based protocols organize all IDs in a tree of ID prefixes [1, 2, 25, 44]. Each in-tree prefix has two child nodes that have one additional bit, '0' or '1'. The tag IDs are leaves of the tree. The RFID reader walks through the tree, and requires tags with matching prefixes to transmit their IDs. Also related is a recent work that identifies tags belonging to a given set [43].

Kodialam and Nandagopal [14] estimate the number of tags in an RFID system based on the probabilistic counting methods [13]. The same authors propose a non-biased follow-up work in [15]. Han et al. [11] improve the performance of [14]. Qian et al. [27] present the Lottery-Frame scheme (LoF) for estimating the number of tags in a multiple-reader scenario. Li et al. [18] uses the maximum likelihood method. Sheng et al. design two probabilistic algorithms to identify large tag groups [32]. For the *size measurement* category, the following problems lack prior study: precisely determining the number of tags, estimating the sizes of all groups, classifying groups based on multiple thresholds, and finding the number of new tags that enter the system and the number of existing tags that depart between two consecutive measurements. In addition, most existing work [14, 15, 27, 32] focuses on time efficiency. Their goal is to reduce the protocol execution time for solving a problem. Energy-efficient protocol design is under-studied.

Tan et al. [33] design a Trust Reader Protocol (TRP) for probabilistic missing-tag detection. Their follow-up work [31] can probabilistically identify missing tags as well as unknown tags in the system. However, it falls short of exact detection because their protocols cannot guarantee all missing tags (or unknown tags) are identified. Luo et al. [22] improves on TRP through sampling. All these protocols are designed for time efficiency, without considering how to improve energy efficiency in the detection process. Bu et al. [3] design efficient protocols to detect and pinpoint misplaced tags in a large warehouse, with the consideration of both time efficiency and energy efficiency. Luo et al. [23] reveal the energy-time tradeoff in the missing tag problem. For the *anomaly detection* category, the following problems lack prior study: exact unknown-tag detection, which is to precisely identify all unknown tags, and mixed detection of missing tags and unknown tags when both exist (probabilistic and exact versions of this problem). Although both missing tags and unknown tags are studied in [31], they are considered separately. It is unclear how their co-existence will affect each other's detection.

The idea of using RFID tags for sensing purpose has been around before [24, 29], but the problem of designing an efficient protocol to collect sensor-produced information from tags is only studied recently in [8, 40], with a primary goal of minimizing the protocol execution time. Qiao et al. [28] propose energy-efficient polling protocols for sensor-augmented RFID systems. The problem of information collection by mobile tags is not studied before.

Weis et al. [36] propose a privacy-preserving authentication protocol, in which the reader has to try all keys in the database in order to see if there exists one that produces a match with the authentication data sent from the tag. The computation overhead is prohibitively high. Yao et al. [39] use a reversible hash function, CuckooHash [10], in their authentication, which is not secure. In the weak privacy model by Lu et al. [21], a tag will keep responding the same key index to any fake readers, until it is refreshed with a new key index after a successful authentication with a legitimate reader. Hence, the key index can be used to identify the tag before refreshment. We show in [17] that all tree-based protocols [9, 19, 20, 39] cannot ensure total privacy protection, either. Therefore, the problem of privacy-preserving authentication remains open.

1.7 Outline of the Book

In Chapter 2, we discuss how to estimate the number of tags in a large RFID system. Solving the tag estimation problem incurs energy cost both at the RFID reader and at active tags. The asymmetry is that energy cost at tags should be minimized while energy cost at the reader is relatively less of a concern. We present two probabilistic algorithms that strive at saving tags' energy. The performance of the algorithms is controlled by a parameter that can be tuned to make tradeoff between energy cost and execution time.

In Chapter 3, we explain how to collect information from a sensor-augmented RFID network. We first give a lower bound on the execution time for any sensor information collection protocol. We point out that the existing ID-collection protocols are ill-fitted for this task. We then present a straightforward polling-based protocol as a baseline for comparison. Its execution time is much larger than the lower bound and its energy cost is also very high. We set forward to present more sophisticated protocols that significantly reduce the execution time toward the lower bound.

In Chapter 4, we discuss how to efficiently collect information from a subset of all tags. We first show that the standard, straightforward polling design is not energy-efficient because each tag has to continuously monitor the wireless channel and receive all tag IDs that the reader needs to collect information from, which is energy-consuming if the number of such tags is large. We show that a coded polling protocol is able to cut the amount of data each tag has to receive by half, which means that energy consumption per tag is also reduced by half. We then present two novel tag-ordering polling protocols that can reduce per-tag energy consumption by more than an order of magnitude when comparing with the coded polling protocol. In these designs, both the time efficiency and the energy efficiency are taken into consideration, whereas the tradeoff between time and energy is revealed.

References

1. Information Technology – Radio Frequency Identification for Item Management Air Interface – Part 6: Parameters for Air Interface Communications at 860-960 MHz. Final Draft International Standard ISO 18000-6 (2003)
2. Bhandari, N., Sahoo, A., Iyer, S.: Intelligent Query Tree (IQT) Protocol to Improve RFID Tag Read Efficiency. Proc. of IEEE ICIT (2006)
3. Bu, K., Xiao, B., Xiao, Q., Chen, S.: Efficient Pinpointing of Misplaced Tags in Large RFID Systems. Proc. of IEEE SECON (2011)
4. Bustillo, M.: Wal-Mart Radio Tags to Track Clothing (2010). URL `http://online.wsj.com/article/SB10001424052748704421304575383213061198090.html`
5. Cha, J.R., Kim, J.H.: Dynamic Framed Slotted ALOHA Algorithms using Fast Tag Estimation Method for RFID Systems. Proc. of IEEE CCNC (2006)
6. Chen, S., Fang, Y., Xia, Y.: Lexicographic Maxmin Fairness for Data Collection in Wireless Sensor Networks. IEEE Transactions on Mobile Computing **6**(7), 762–776 (2007)
7. Chen, S., Yang, N.: Congestion Avoidance based on Lightweight Buffer Management in Sensor Networks. IEEE Transactions on Parallel and Distributed Systems **17**(9), 934–946 (2006)
8. Chen, S., Zhang, M., Xiao, B.: Efficient Information Collection Protocols for Sensor-augmented RFID Networks. Proc. of IEEE INFOCOM (2011)
9. Dimitriou, T.: A Secure and Efficient RFID Protocol that Could Make Big Brother (partially) Obsolete. Proc. of IEEE PerCom (2006)
10. Erlingsson, Ú., Manasse, M., McSherry, F.: A Cool and Practical Alternative to Traditional Hash Tables. Proc. of WDAS (2006)
11. Han, H., Sheng, B., Tan, C.C., Li, Q., Mao, W., Lu, S.: Counting RFID Tags Efficiently and Anonymously. Proc. of IEEE INFOCOM (2010)
12. Hollinger, R., Davis, J.: National Retail Security Survey (2001). URL `http://diogenesllc.com/NRSS_2001.pdf`
13. Hwang, K., Vander-Zanden, B., Taylor, H.: A Linear-time Probabilistic Counting Algorithm for Database Applications. ACM Transactions on Database Systems **15**(2) (1990)
14. Kodialam, M., Nandagopal, T.: Fast and Reliable Estimation Schemes in RFID Systems. Proc. of ACM MOBICOM (2006)
15. Kodialam, M., Nandagopal, T., Lau, W.: Anonymous Tracking Using RFID tags. Proc. of IEEE INFOCOM (2007)
16. Lee, S., Joo, S., Lee, C.: An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification. Proc. of IEEE MOBIQUITOUS (2005)
17. Li, T., Luo, W., Mo, Z., Chen, S.: Privacy-preserving RFID Authentication based on Cryptographical Encoding. Proc. of IEEE INFOCOM (2012)
18. Li, T., Wu, S., Chen, S., Yang, M.: Energy Efficient Algorithms for the RFID Estimation Problem. Proc. of IEEE INFOCOM (2010)
19. Lu, L., Han, J., Hu, L., Liu, Y., Ni, L.: Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems. Proc. of IEEE PerCom (2007)
20. Lu, L., Han, J., Xiao, R., Liu, Y.: ACTION: Breaking the Privacy Barrier for RFID Systems. Proc. of IEEE INFOCOM (2009)
21. Lu, L., Liu, Y., Li, X.: Refresh: Weak Privacy Model for RFID Systems. Proc. of IEEE INFOCOM (2010)
22. Luo, W., Chen, S., Li, T., Chen, S.: Efficient Missing Tag Detection in RFID Systems. Proc. of IEEE INFOCOM, mini-conference (2011)
23. Luo, W., Chen, S., Li, T., Qiao, Y.: Probabilistic Missing-tag Detection and Energy-Time Tradeoff in Large-scale RFID Systems. Proc. of ACM MobiHoc (2012)
24. Miura, M., Ito, S., Takatsuka, R., Sugihara, T., Kunifuji, S.: An Empirical Study of an RFID Mat Sensor System in a Group Home. Journal of Networks **4**(2) (2009)
25. Myung, J., Lee, W.: Adaptive Splitting Protocols for RFID Tag Collision Arbitration. Proc. of ACM MOBIHOC (2006)

26. Ni, L.M., Liu, Y., Lau, Y.C., Patil, A.: LANDMARC: Indoor Location Sensing using Active RFID. ACM Wireless Networks (WINET) **10**(6) (2004)
27. Qian, C., Ngan, H., Liu, Y.: Cardinality Estimation for Large-scale RFID Systems. Proc. of IEEE PerCom (2008)
28. Qiao, Y., Chen, S., Li, T., Chen, S.: Energy-efficient Polling Protocols in RFID Systems. Proc. of ACM MobiHoc (2011)
29. Ruhanen, A., Hanhikorpi, M., Bertuccelli, F., Colonna, A., Malik, W., Ranasinghe, D., Lopez, T.S., Yan, N., Tavilampi, M.: Sensor-enabled RFID Tag Handbook. BRIDGE, IST-2005-033546 (2008)
30. Sarangan, V., Devarapalli, M.R., Radhakrishnan, S.: A Framework for Fast RFID Tag Reading in Static and Mobile Environments. The International Journal of Computer and Telecommunications Networking **52**(5) (2008)
31. Sheng, B., Li, Q., Mao, W.: Efficient Continuous Scanning in RFID Systems. Proc. of IEEE INFOCOM (2010)
32. Sheng, B., Tan, C.C., Li, Q., Mao, W.: Finding Popular Categories for RFID Tags. Proc. of ACM MOBIHOC (2008)
33. Tan, C., Sheng, B., Li, Q.: How to Monitor for Missing RFID Tags. Proc. of IEEE ICDCS (2008)
34. Vogt, H.: Efficient Object Identification with Passive RFID Tags. Proc. of IEEE PerCom (2002)
35. Want, R.: An Introduction to RFID Technology. Proc. of IEEE PerCom (2006)
36. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. Lecture Notes in Computer Science — Security in Pervasive Computing **2802** (2004)
37. Wikipedia: Radio-frequency identification (Mar 2012). URL `http://en.wikipedia.org/wiki/Radio-frequency_identification`
38. Wolverton, J.: Wal-Mart to Embed RFID Tags in Clothing Beginning August 1 (2010). URL `http://www.thenewamerican.com/index.php/tech-mainmenu-30/computers/4157-wal-mart-to-embed-rfid-tags-in-clothing-beginning-august-1`
39. Yao, Q., Qi, Y., Han, J., Zhao, J., Li, X., Liu, Y.: Randomizing RFID Private Authentication. Proc. of IEEE PerCom (2009)
40. Yue, H., Zhang, C., Pan, M., Fang, Y., Chen, S.: A Time-efficient Information Collection Protocol for Large-scale RFID Systems. Proc. of IEEE INFOCOM (2012)
41. Zhang, M., Li, T., Chen, S., Li, B.: Using Analog Network Coding to Improve the RFID Reading Throughput. Proc. of IEEE ICDCS (2010)
42. Zhen, B., Kobayashi, M., Shimizu, M.: Framed ALOHA for Multiple RFID Objects Identification. IEICE Transactions on Communications (2005)
43. Zheng, Y., Li, M.: Fast Tag Searching Protocol for Large-Scale RFID Systems. Proc. of IEEE ICNP (2011)
44. Zhou, F., Chen, C., Jin, D., Huang, C., Min, H.: Evaluating and Optimizing Power Consumption of Anti-collision Protocols for Applications in RFID Systems. Proc. of ISLPED (2004)