Managing RFID Data: Challenges, Opportunities and Solutions

Lei Xie, *Member, IEEE*, Yafeng Yin, *Student Member, IEEE*, Athanasios V. Vasilakos, *Senior Member, IEEE*, and Sanglu Lu, *Member, IEEE*

***Abstract*—The advances of Radio-Frequency Identification (RFID) technology have significantly enhanced the capability of capturing data from pervasive space. It becomes a great challenge in the information era to effectively understand human behavior, mobility and activity through the perceived RFID data. Focusing on RFID data management, this article provides an overview of current challenges, emerging opportunities and recent progresses in RFID. In particular, this article has described and analyzed the research work on three aspects: algorithm, protocol and performance evaluation. We investigate the research progress in RFID with anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings. We emphasize the basic principles of RFID data management to understand the state-of-the-art and to address directions of future research in RFID.**

***Index Terms*—RFID, data management, anti-collision algorithms, authentication and privacy protection, localization and activity sensing, performance evaluation.**

I. Introduction

AS A TECHNOLOGY for automated identification of objects, RFID (Radio-Frequency IDentification) has gained significant momentum in the past few years. Recently RFID has been more and more frequently introduced in applications like retail and distribution, target monitoring and tracking, etc, as elaborated in literatures [1], [2], and [3]. The most important reason of such phenomenon is that, by leveraging the RFID technology, we are able to embed the intelligence into each physical object in a low-cost approach. In this way, the "passive intelligence" is effectively realized in the ubiquitous space, which can be regarded as a right candidate for green communications [4][5]. As such a novel technology, RFID has provided us with 1) the capability to uniquely identify the objects in the physical world and 2) a passive, battery-free interconnection mechanism. Furthermore, the dropping tag costs and vigorous RFID standardization have accelerated the wide-spread usage of the RFID technology.

Manuscript received May 8, 2013; revised November 15, 2013. L. Xie, Y. Yin, and S. Lu are supported in part by National Natural Science Foundation of China under Grant No. 61100196, 61321491, 91218302; JiangSu Natural Science Foundation under Grant No. BK2011559; Key Project of Jiangsu Research Program under Grant No. BE2013116; EU FP7 IRSES MobileCloud Project under Grant No. 612212. Lei Xie is the corresponding author.

L. Xie, Y. Yin, and S. Lu are with the State Key Laboratory for Novel Software Technology, Nanjing University, China (e-mail: lxie@nju.edu.cn, yyf@dislab.nju.edu.cn, sanglu@nju.edu.cn).

A. Vasilakos is with University of Western Macedonia, Greece (e-mail: vasilako@ath.forthnet.gr).

Digital Object Identifier 10.1109/SURV.2014.022614.00143

In conventional RFID applications, the items are attached with RFID tags and densely placed in a large scale. The RFID tag is a small mircochip attached with an antenna in a package. During the scanning process, the RFID reader powers up and transmits a continuous wave to energize the tags. The tag then responds to the reader with tag-carried information by modulating the backscattered signals. The reader further decodes the signal and obtains the corresponding information [6][7][8]. In this way, the RFID system can not only "identify" but also "locate" the labeled item, by providing the information including the "identity" as well as the "location". Here, the "identity" is precise information extracted from the tag, while the "location" is usually inaccurate information estimated according to environmental parameters. Furthermore, these RFID applications often involve lots of human activities, in order to precisely understand human behavior, mobility and activity through the perceived RFID data, it is essential to effectively manage RFID data to extract the useful information, while ensuring the overall performance. How to effectively manage RFID data? As a matter of fact, several properties are essentially required for effective RFID data management. We elaborate on these properties as follows:

- Efficiency: while interrogating a number of tags, two metrics are highly pertinent to efficiency, i.e., time efficiency to reduce the total scanning time, and energy efficiency to reduce the total power consumption.
- Trustworthy: the communication between the reader and tags should be both privacy-preserving and anti-counterfeiting.
- Localizability: the objects or people should be accurately located within the specified range of time delay.
- Reliability: in realistic settings, the RFID system should be able to tackle with issues like signal interference, multi-path effect and energy absorption.

These properties basically belong to the nonfunctional requirements for RFID systems. According to the above descriptions, it is essential to provide some mechanisms to effectively satisfy the above nonfunctional requirements. Therefore, several new research topics are necessarily to be addressed for RFID data management. Specifically, they include anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings. Fig. 1 illustrates these research topics corresponding to the above properties. In fact, these research topics are not independent of each other, but are correlated with each other. Besides, since these topics

mainly focus on different layers of the protocol stack, the relationship between these topics and the protocol stack is also shown in the figure. This figure provides us a clear structured framework of these research topics.

The main contributions of this article are summarized as follows:

- We investigate the current challenges and emerging opportunities in managing RFID data, and provide some guidance and substantial lessons learned in the research of RFID data management.
- We emphasize the basic principles of RFID data management to understand the state-of-the-art research achievements. Furthermore, we present comparative studies over existing approaches to analyze their features specifically and concretely.
- We provide a long term vision for future research directions, with more emphasis on insights into future challenges and opportunities in RFID research.

The rest of this article is organized as follows. We first present the challenges and opportunities for RFID data management in Section II. We then respectively introduce the research progresses of anti-collision algorithms, authentication and privacy protection protocols, as well as localization and activity sensing in Section III, IV, and V. After that, in Section VI we further provide a summative discussion from a more realistic perspective, i.e., performance tuning in realistic settings. We envision the future research directions in Section VII and conclude in Section VIII.

II. Challenges and Opportunities for RFID Data Management

Compared to the other intelligent systems like two-dimension code, sensor network, etc., the current design of RFID system has provided us the following opportunities for effective RFID data management [9]:

1) RFID tags can be automatically identified in a non-contact approach.
2) RFID tag contains a certain number of logical gates, which support simple logical processing in the tag side.
3) RFID tag is able to store some data permanently in its tiny on-board memory.
4) The backscattered signal from RFID tag has properties like any other wireless devices, e.g., the received signal strength (RSS).
5) RFID tag is very cheap, which makes the large scale-deployment become possible.

Nevertheless, there exist some significant challenges that must be overcome before the benefits are realized. The major challenges of managing RFID data are summarized as follows:

1) The communication link between the RFID reader and the tag is not stable, which is susceptible to issues like signal interference, multi-path effect and energy absorption. Unlike those battery-powered systems, the passive RFID system is especially vulnerable to the ambient noises and interferences due to the backscatter property. For example, the missed reading phenomenon is very common for RFID systems even in a relatively ideal situation close to free space. How to deal with the unstable communication is really a challenging problem for passive RFID systems.
2) Due to the scarce resource in the tag side, the logical processing in the tag is required to be simple enough, the storage requirement in the tag should be limited to several kilobytes. Therefore, it is actually very difficult to implement comprehensive and powerful functions in the RFID systems while satisfying the scarce resource constraint.
3) There already exists an industry standard ISO 18000-6C (also known as EPC Class 1 Generation 2) which specifies how RFID readers identify and read RFID tags, the design of protocols and algorithms over RFID systems should conform to the standard, or at least be subject to minor changes. In contrast with the other wireless devices like sensor nodes, smart phones, etc, since the chips in the tags conventionally cannot be reprogrammed, the only part we can freely reprogram is the RFID reader, still the standard should be conformed. Any solutions which requires to substantially change the tag's execution logics are considered to be impractical for RFID systems.

TABLE I
Challenges and Opportunities for RFID Data Management
(C denotes Challenges, O denotes Opportunities)

	PHY Layer	MAC Layer	APP Layer
Anti-collision Algorithm		**C**:(2),(3) **O**:(2)	**C**:(2) **O**:(2)
Authentication & Privacy Protection	**O**:(1),(4)		**C**:(2),(3) **O**:(2),(3)
Localization & Activity Sensing	**C**:(1) **O**:(4)		**O**:(1),(5)
Performance Tuning in Realistic Settings	**C**:(1)	**C**:(3)	

Therefore, in order to effectively investigate into the techniques of managing RFID data, one intuitive thinking is to sufficiently leverage the potential opportunities to overcome the emerging challenges. In order to distinguish these opportunities and challenges more closely, Table I has categorized the above challenges and opportunities according to the research topics and involved layers in the protocol stack. In this way, we can get a better understanding of how to deal with these challenges and opportunities.

III. Anti-collision Algorithms in RFID Systems

In conventional RFID applications, a large number of RFID tags are widely deployed in the specified regions. In order to identify these tags in a fast approach, it is essential for the RFID reader to utilize an anti-collision algorithm to effectively read these tags one by one. In wireless environment, conventional wireless devices mainly leverage CSMA/CA to realize the communication among multiple devices, e.g., the 802.11 protocol series. Being different from the conventional wireless devices, the RFID tag is a rather simple wireless device with scarce resource. The tags are unable to self-regulate their radio transmissions to avoid collisions. Specifically, the tag does not have enough processing capacity and energy to realize the above competition mechanisms to avoid transmission

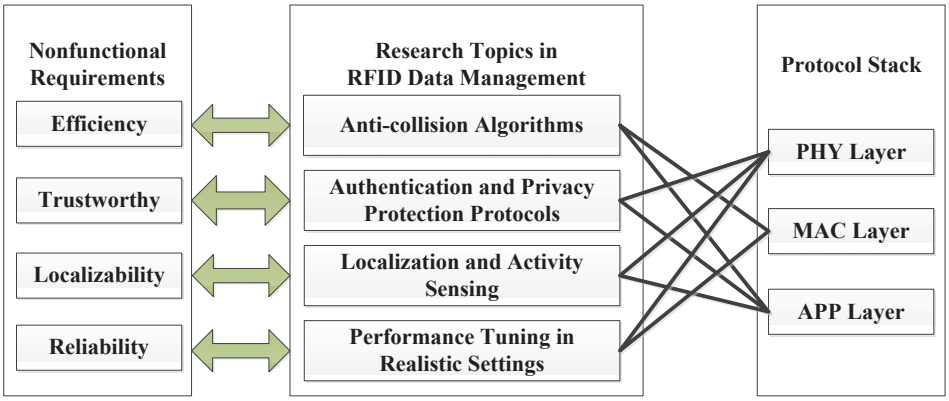


Fig. 1. New Research Topics in RFID Data Management

collisions. Therefore, effective anti-collision algorithms should be customized for RFID systems. Klair et al. provided an overview of RFID anti-collision protocols [10]. Here, to be more specifically, we further classify and elaborate the principles of the most recent research progresses. In the following subsections, we first introduce the anti-collision algorithms in tag identification, then, two kinds of ingenious techniques are respectively introduced, i.e., estimating the tag size and polling the tags based on the anti-collision algorithms.

A. Tag Identification

In regard to the features of RFID system, an effective tag identification protocol is expected to have the following properties: 1) Simple: the processing logic of the protocol (including the execution flow and the state transition) should be as simple as possible, due to the scarce resource in the tag; 2) Efficient: when interrogating a large number of tags, the protocol should provide a light-weight communication mechanism to avoid unnecessary transmissions of control messages. In this way, the high throughput and low transmission delay can be guaranteed.

The current anti-collision algorithms can be divided into two categories: the tree based anti-collision algorithms [11, 12] and the slotted ALOHA based anti-collision algorithms [13–18]. The former leverages the binary search tree to divide the collided tag set into two subsets in a recursive approach. In regard to those tag sets with opportunities of collisions, the "keeping silent" mechanism is used to resolve the collision problems. The method to divide the sets is comprised of the random binary tree algorithms and the query binary tree algorithms. Myung et al. [11] proposed an adaptive tree-based anti-collision algorithm to efficiently identify the tags. Pan et al. [12] proposed a smart tree traversal mechanism based on the query tree, which conducts the tag identification with low delay.

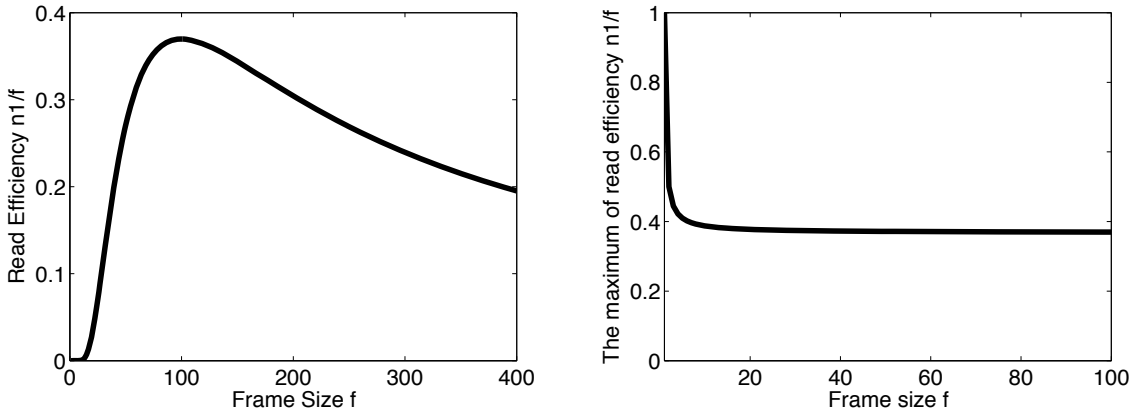
The ALOHA protocol is first used for random access in packet radio network. In order to improve the efficiency of tag identification in RFID systems, the slotted ALOHA protocol [13, 14] is proposed to effectively resolve the collisions. The slotted ALOHA protocol combines a certain number of time slots into a "frame". During the interrogation, the reader sends a continuous wave to energize all tags in the effective scanning range. At the beginning of each frame, the reader broadcasts the frame size f to the surrounding tags, i.e., the number of slots in the following frame. After each tag receives the frame size f, it randomly selects a slot from the 1st slot to the fth slot in this frame and responds to the reader. If the tag successfully responds, i.e., no collision happens in the selected slot, then the specified tag is kept silent in the following query rounds; otherwise, the tag will continue to select another slot in the next frame to resend the ID. Therefore, there exists one of the following situations for each slot within the frame: 1) empty slot: no tag responds in this slot; 2) singleton slot: only one unique tag responds in this slot; 3) collision slot: multiple tags respond in this slot. Each kind of slot gives different information. Currently, the slotted ALOHA protocol has been adopted in the EPC C1G2 standard.

TABLE II
COMPARATIVE STUDY OF THE TWO KINDS OF ANTI-COLLISION ALGORITHMS

	Binary tree-based anti-collision algorithms	**Slotted ALOHA-based anti-collision algorithms**
Advantages	Normally deterministic algorithm is used. The query tree-based algorithms do not require to store the intermediate state variable.	The randomized algorithm is used with a good performance on average. The randomization makes the results over slots meet a certain probability distribution, facilitating various statistical analysis.
Disadvantages	For the query tree-based algorithms, the delay for tag identification is subject to the length and distribution of tag IDs.	The randomness of the algorithm makes the "starvation problem" possible, some tags can never select a singleton slot to respond. In the worst case, the delay approaches $+\infty$.

In Table II, we respectively compare the two kinds of anti-collision algorithms in terms of advantages and disadvantages. Generally speaking, there are pros and cons to both kinds of algorithms.

In regard to the slotted ALOHA protocol, the frame size for each query round is of crucial importance to the overall performance for identification. For a given tag set, if the frame size is too large, then most of the slots in this frame will be empty slots, causing the waste of slots; if the frame size



(a) (b)

Fig. 2. (a) Given the tag size $n = 100$, the relationship between the read efficiency $\frac{n_1}{f}$ and the frame size f. (b) As the tag size n varies, the maximum read efficiency obtained when $f^* = n$.

is too small, then there will exist transmission collisions for most of the slots, causing most tags to retransmit in the next query round. Hence, the frame size should be dynamically adjusted according to the number of tags in the current query round. Therefore, many researchers have investigated into this problem. Schoute et al. analyze the impact of the dynamic frame size selection on the reading performance in slotted ALOHA protocol [15]. Floerkemeier et al. propose the strategy of optimizing the dynamic frame size, according to the Bayesian probability model [16]. Vogt et al. leverage Markov process to model the identification process, and calculate a series of the optimized frame sizes during the interrogation process [17].

Lee et al. further derive the optimal dynamic frame sizes to maximize the channel efficiency [18]. Their research conclusions indicate that, if the frame size used in each query round is equivalent to the number of tags to be identified, then the maximum efficiency can be achieved for the channel. The detail principle is described as follows: assume the current number of tags within the effective scanning range is n, the frame size is f. As the number of tags in each slot conforms to the Binomial distribution, then, the expected number of singleton slots in this frame is $E[n_1] = n \times (1-1/f)^{n-1}$. In order to maximize the channel efficiency $\frac{n_1}{f}$, i.e., the ratio of the number of singleton slots to the frame size, we get the value of f through the extremum of $\frac{n_1}{f}$: $\frac{\partial E[n_1]/f}{\partial f} = 0 \rightarrow f^* = n$, then the maximum channel efficiency is $n_1/f^* \rightarrow 1/e$. In Fig.2(a) and Fig.2(b), we provide more detail descriptions for the above properties. Fig.2(a) depicts the impact of the frame size f on the channel efficiency, when the tag size $n = 100$. Note that as the frame size gradually increases from 1 to 400, the read efficiency gradually increases to the maximum value $\frac{1}{e}$ and then decreases. The maximum efficiency is achieved when $f = 100$. Fig.2(b) depicts the impact of the tag size n on the channel efficiency, when the optimal frame size $f^* = n$ is used. Note that when the value of n is small, the optimal efficiency is larger than $\frac{1}{e}$, e.g., when the tag size $n = 1$, the optimal efficiency is 100% if the frame size is set to 1. As the value of n gradually increases, the optimal efficiency quickly converges to $\frac{1}{e}$. It implies that, the local optimal read efficiency in a query round approaches to $\frac{1}{e}$ when $n > 5$, if the optimal frame size $f^* = n$ is used. If this strategy is used for each query round, then the overall efficiency is close to $\frac{1}{e}$. Since $\frac{1}{e}$ is the upper bound of the overall efficiency, then the global optimal efficiency is also achieved with this strategy.

The above anti-collision algorithms are conventionally devised towards fairly idealized settings, without sufficiently addressing the difficulties in real applications, e.g., the frequent movement of tags, the signal interference among multiple RFID readers, the signal attenuation and multi-path effect, etc. Therefore, a few research work start to focus on and try to solve the above problems. Due to the limited scanning range of a single RFID reader, multiple readers are conventionally deployed in the application scenarios. Since the former research work mainly focus on resolving the collisions among multiple tag transmissions, without considering the signal interference problem among multiple readers, literature [19, 20] propose optimized activating and scheduling schemes for multiple readers. In this way, multiple readers are able to collaboratively avoid the signal transmission collisions. Furthermore, by utilizing the mobile RFID reader, Sheng et al. develop efficient schemes for continuous scanning operations defined in both spatial and temporal domains [21]. Their basic idea is to fully utilize the information gathered in the previous scanning operations to reduce the scanning time of the succeeding ones. The former research work mainly devise optimized schemes to identify statically deployed tags in fairly idealized settings, without considering the impact of some ubiquitous issues like path loss in the mobile environment. In regard to this problem, Xie et al. propose a probabilistic model for RFID tag identification [22], according to the continuous changing properties of signal attenuation. Based on this model, they devise optimal parameters for the tag identification, which conforms to the EPC Gen2 standard. Moreover, in order to execute the continuous scanning with mobile reader for tag identification in realistic settings, Xie et al. conduct comprehensive experimental study on mobile RFID reading, and design very efficient algorithms to maximize the time-efficiency and energy-efficiency by skillfully adjusting the readers power and moving speed [23]. In order to identify

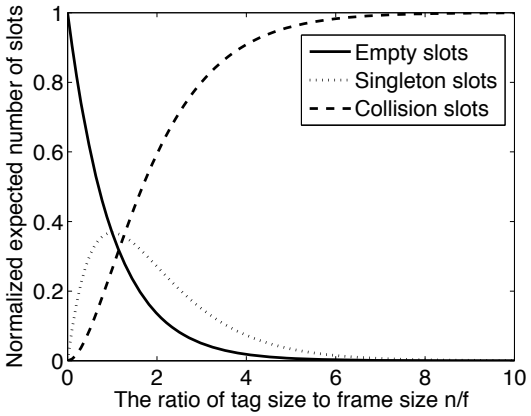


Fig. 3. The normalized expected number of empty/singleton/collision slots as the ratio of $\frac{n}{f}$ varies

the RFID tags towards the specified area, Yin et al. propose a "focus and shoot" method for efficient tag identification, based on extensive empirical study on RFID systems [24].

B. Estimating the Tag Size

With the further extension of RFID applications, a number of applications only require some statistical information for data analysis and mining. In this situation, the RFID system only requires to quickly estimate the statistics, instead of identifying the tags one by one. One of the most important statistics is the tag size, i.e., the overall number of tags. Moreover, the slotted ALOHA protocol based on dynamic frame sizes also requires to estimate the current tag size for determining the frame size. Therefore, recently there are many research work which focus on how to fast and accurately estimate the overall tag size. The core idea is as follows: since the slotted ALOHA protocol requires the tags to randomly select the slots to respond inside the frame, then it is possible to leverage the statistics regularities in the randomized algorithm to estimate the tag size. Specifically, according to the current protocol in EPC Gen 2 standard, the number of empty slots, singleton slots and collision slots actually conform to the Binomial distribution in a statistical approach. When the number of samplings for slots is large enough, the number of tags can be effectively estimated according to the Binomial distribution.

Based on the above idea, Kodialam et al. propose a fast and reliable estimation mechanisms for tag size in a practical approach [25]. The major idea is as follows: assume in a certain query round with fixed frame size f, as the overall number of tags n increases, the number of empty slots is expected to decrease, the number of collision slots is expected to increase, while the number of singleton slots is expected to first increase and then decrease. Therefore, the number of empty slots (collision slots) is monotonically decreasing (increasing) with the overall number of tags. Fig.3 depicts the normalized expected number of empty/singleton/collision slots as the ratio of $\frac{n}{f}$ varies, here the number of slots is normalized to a real number in the range 0 through 1 by dividing the frame size f. Based on the probabilistic model of Binomial distribution, the authors present unified estimation algorithms according to the empty slots and collision slots, and they further reduce the estimation errors through repeated sampling.

TABLE III
COMPARISON OF ALGORITHMS FOR TAG SIZE ESTIMATION

Estimation Algorithm	Compatibility with Slotted ALOHA	Indicator for Estimation	Probability Model
[25]	Compatible	The number of empty and collision slots	Binomial distribution
[26]	Compatible	The number of empty, singleton and collision slots	Posterior probability model based on binomial distribution
[27]	Compatible	The first slot with tag response	Binomial distribution
[28][29]	Not Compatible	The fringe of collision slots	Geometric distribution
[30]	Compatible	The average run-length of ones in the bit string received	Binomial distribution

Although the number of singleton slots is not monotonic to the overall tag size, the tag size cannot be estimated purely from the number of singleton slots, nevertheless, the number of three kinds of slots together can help to estimate the tag size in a more accurate approach. Hence, Chen et al. present a posterior probability model based on the observed number of empty/singleton/collision slots [26]. They propose an accurate tag estimate method by maximizing the posterior probability.

The above mechanisms all require a large number of samplings over the three kinds of slots to improve the estimation accuracy. In fact, some other properties can be leveraged to accurately estimate the tag size in a faster approach. Han et al. propose an efficient and anonymous scheme for tag size estimation [27], which leverages the position of the first reply from a group of tags in a frame. Moreover, in order to tackle with the multiple reading problem, i.e., one single tag can be interrogated multiple times with multiple readers, Chen et al. present a replicate-insensitive estimation scheme [28], which eliminates the multiple reading in multi-reader scenarios. The authors further propose an adaptively splitting-based arbitration protocol [29]. This protocol requires a single tag to select multiple slots in a frame to respond, according to the Geometric distribution. Specifically, each tag have a probability of $\frac{1}{2^t}$ to respond in the $t-1$th slot. Then, the tag size can be effectively estimated according to the fringe of collision slots in the frame. Shahzad et al. propose a new scheme for estimating tag population size called average run based tag estimation [30]. The technique is based on the average run-length of ones in the bit string received using the standardized framed slotted ALOHA protocol. It is easy to deploy because it neither requires modification to tags nor to the communication protocol between tags and readers. Table III provides a comparison of the above algorithms for tag size estimation.

Instead of simply estimating the tag size, a number of researchers start to investigate how to realize more complicated data analysis and mining over RFID systems. Sheng et al. consider the problem of identifying popular categories of

RFID tags out of a large collection of tags, without reading all the tag data [31]. They propose effective algorithms based on the idea of group testing, which can efficiently derive popular categories of tags. Kodialam et al. propose a privacy-preserving estimation mechanism over dynamically moving tags in applications like object tracking [32]. This mechanism can fast count the number of tags moving from location A to B during the time interval (t_1, t_2). In this way, the traffic can be effectively tracked without exactly reading the tag IDs. In general, research work in this area are relatively rare. With the further extension of RFID applications, efficient techniques for data analysis and mining over RFID systems will attract widespread attentions and in-depth studies.

C. Polling the Tags

Instead of obtaining all tags' IDs in the effective scanning range, some applications only require to poll the tags in a specified tag set, verifying whether these tags are missing. For example, in regard to the applications like warehouse management, assume that each of the goods is attached with an RFID tag with unique ID, the administrator should check the specified inventories according to the list of goods. In this situation, it becomes an essential problem to devise efficient polling protocols over the RFID tags, such that both the time efficiency and energy efficiency can be achieved. A straightforward solution is to realize the following "roll call" mechanism: the reader continuously broadcasts the tags' IDs according to the check list. After each tag ID is broadcasted, the reader will wait for the specified tag to return a short response. If a short response is obtained, then it implies that this tag exists in the scanning range; otherwise, this tag is expected to be missing. However, there are a number of disadvantages for the above mechanism: 1) it is not compatible with the slotted ALOHA; 2) the transmission delay of the tag ID with 96 bits is fairly large, the efficiency is greatly reduced. Therefore, many researchers have investigated into this problem, and tried to design efficient polling protocols based on the slotted ALOHA, aiming to sufficiently reduce the overall scanning time.

Note that during each query round of the interrogation, each of the activated tags will "randomly" select a slot to respond inside the frame. However, due to the simplicity of the tag's design, it is rather difficult to realize the "pure randomness". Instead, the "pseudo randomness" is used as follows: For each query round the reader first broadcasts a random number r to the tags. After that, each of the activated tags will compute a pseudo random number s as the selected slot number, here $s = hash(ID, r) mod\ f$, ID and f respectively denote the tag ID and frame size. The above "pseudo randomness" implies that, in regard to a specified tag, once the random number r and the frame size f is set, the corresponding slot selected by this tag inside the frame is determined. This property makes it possible for efficient polling over the tags. Since the tag IDs in the specified tag set can be known in advance, then before interrogating the tags, the reader can precompute the expected state for each slot accordingly. The expected state for each slot can be empty slot, singleton slot or collision slot. Therefore, in regard to a specified slot, if this slot is expected to be singleton/collision slot but turns out to be empty, then it implies that the tag(s) mapping to this slot is(are) missing. Fig.4 gives an example of the polling mechanism. As the figure shows, the dotted box denotes the missing tag, while the solid box denotes the existing tag. Assume that the tag E, F and H are missing, if the corresponding slots turn out to be empty, then the tags can be determined missing. However, if the tag C is missing, the corresponding slot still turns out to be collision slot due to the existence of the tag B and D. In this situation, the tag C cannot be identified as missing, resulting in the false positive error. The above polling mechanism provides a theoretical foundation to recent research work.

Based on the above understanding, Li et al. study a practically important problem of monitoring a large set of RFID tags, i.e., efficiently identifying the missing tags in a large RFID system [33]. Based on the "pseudo randomness", they design a series of missing-tag identification protocols that employ novel techniques to reduce the execution time. In order to deal with the problem of collecting real-time information from a set of battery-powered active tags, Qiao et al. propose a tag-ordering polling protocol [34] that can reduce per-tag energy consumption by more than an order of magnitude. Moreover, they apply partitioned Bloom filters to further enhance the performance, such that it can achieve much better energy efficiency without degradation in protocol execution time. Chen et al. respectively propose a single-hash and a multi-hash based information collection protocol to address the above problem [35], which dramatically reduces the expected execution time. In order to meet the requirement of prompt and reliable batch authentications in large scale RFID applications, Yang et al. propose an identification-free batch authentication protocol based on the polling mechanism [36]. Conventionally, in order to authenticate a large number of tags, the reader should identify and authenticate the tags one by one, which requires a large amount of scanning time. Based on the "pseudo randomness", this batch authentication protocol greatly reduces the overall scanning time, while guaranteeing the probability of false positive error to be below the specified threshold. Being different from the above research work, which mainly poll over all tags in the scanning area, Zheng et al. address the problem of fast searching a particular subset in a large number of RFID tags [37]. They utilize Bloom filter-based compact approximators to efficiently aggregate and exchange the tag information with a two-phase approximation protocol, which significantly reduces the searching time. Generally speaking, these polling mechanisms mainly leverage the pseudo randomness in the slotted ALOHA protocol to effectively reduce the additional cost of uniquely identifying the tags. Nevertheless, since there exist the false positive errors for the polling mechanisms, optimized algorithms are proposed to reduce the probability of false positive errors.

D. Summing Up Challenges and Opportunities

According to the above recent research progress, we summarize the challenges and opportunities for anti-collision algorithms in Table IV, respectively for the tag identification, estimating the tag size, as well as polling the tags.

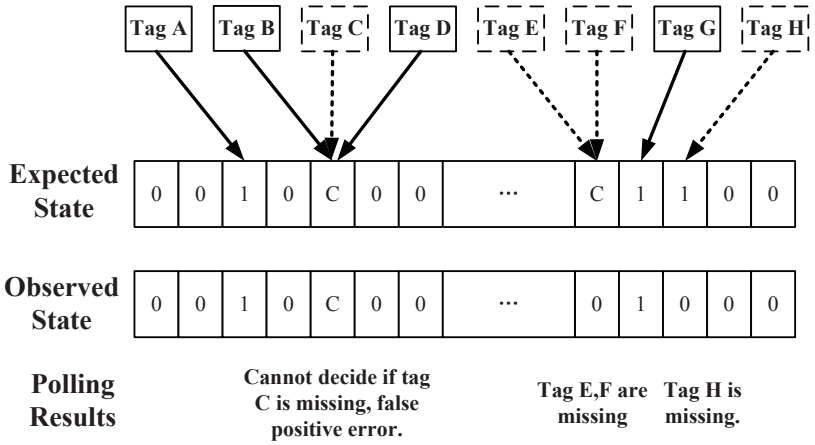


Fig. 4. An example of the polling mechanism in slotted ALOHA-based protocol

TABLE IV
CHALLENGES AND OPPORTUNITIES FOR ANTI-COLLISION ALGORITHMS

Mechanism	Challenges	Opportunities
Tag Identification	Ensuring time-efficiency in realistic situations.	Dynamically adjusting the parameters like the reader's power, the scanning angle, and the frame size can effectively improve the actual performance.
Estimating the Tag Size	Ensuring both the accuracy and the time-efficiency for estimation.	The regular probability distribution in Monte Carlo method contributes to accurate estimation.
Polling the Tags	Ensuring time-efficiency while reducing false-positive/negative errors.	Pseudo randomness can be leveraged for effective polling.

IV. AUTHENTICATION AND PRIVACY PROTECTION PROTOCOLS

The premise of efficient RFID data management is to guarantee the security and privacy of RFID data. The threats of RFID systems mainly come from the unauthorized access to the tags and the existence of counterfeit tags. Specifically, the security problem is how to effectively authenticate the tags when there exist counterfeit tags; the privacy problem is how to prevent the illegal access from the readers to preserve the users' privacy.

For conventional solutions in network security, there are already some encryption and decryption algorithms like DES, AES, RSA and ECC. They can implement functions like encryption and authentication, such that the illegal access, spoofing, eavesdropping and replay attack can be effectively resisted. However, they require a large number of logic processing units on the chip, e.g., AES requires about 20000∼30000 logic gates, whereas RSA and ECC require more logic gates to implement their functions.

Due to the low cost limitation of RFID tags, conventionally one RFID tag can only have 5000∼10000 logic gates. Moreover, these logic gates are mainly used to implement the basic functions of the tag, leaving very few gates for the security functions. Besides, the tag's on-board memory is also rather limited, conventionally the EPC memory can only store 96 bits, while the user memory can only store 512 bits. Hence, the tag's scarce resource cannot support the implementation of the above encryption and decryption operations. Therefore, the greatest challenge to the security and privacy protection in RFID systems lies in how to implement the authentication and privacy protection protocols in a lightweight approach. In the following subsections, we elaborate more on the related research work respectively in physical mechanism-based solutions, symmetric-key encryption-based solutions, and hash function-based solutions.

A. Physical Mechanism-based Solutions

The privacy problem of RFID system is caused by the lack of authentication when the RFID reader interrogates the tags. Without the privacy protection, any RFID reader can privately interrogate the surrounding tags to obtain their ID. In regard to those encrypted tags which cannot be directly identified, they can still be tracked by the illegal readers according to the backscattered encrypted messages. In order to protect the users' privacy in RFID systems, a straightforward approach is to utilize the physical mechanism-based solutions, which mainly include tag killing, electrostatic screening, active jamming and blocking.

The tag killing is actually a brute-force operation. In order to prevent a tag from illegal eavesdropping, the reader simply deactivates a tag by sending a "kill" command with a tag-specific PIN. When a tag receives a "kill" command from the reader, it renders itself permanently inoperative. In this respect, the killing operation leads to loss of primary functions for RFID tags, while preventing arbitrary interrogation and tracking from illegal users, since "dead tags tell no tales". Apparently, it is not a very reasonable solution to completely deactivate a tag. Sarma et al. propose a solution to partially erase the unique part of identification code while keeping the other part including the category ID [38]. In this way, the tag can be prevented from being tracked, while sacrificing the unique identification. Inoue et al. propose to use a new identification code to replace the former code for unique identification [39]. The former identification code can be reactivated when the tag is recycled. In consideration of reusing the tags, the

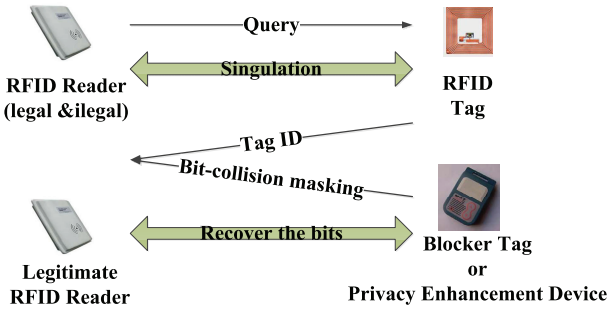


Fig. 5. The framework for the jamming/blocking-based protocols

"sleep" mechanism [39] can be used to render the tags only temporarily inactive. The tag can be appropriately "waked up" when it is needed.

The electrostatic screening is to place the tag into a container which can physically screen the tags from interrogation. This mechanism needs an additional device like Faraday cage [40] as a shield against the electromagnetic coupling. Active jamming uses a device to actively broadcast the interfering signals to prevent the unauthorized read-write operations over tags. Lim et al. propose an active jamming mechanism relying on masking of the identifier at the PHY layer [41]. In their cross-layer framework, the bit-collisions are induced between the backscattered tag identifier and a protective mask, such that a legitimate reader can be allowed to recover the tag identifier but an illegitimate party would not be able to do so. The blocking method uses a special blocking tag to prevent unwanted scanning of tags, by exploiting the anti-collision protocol. Juels et al. propose the above idea of blocking tag based on the tree-based anti-collision protocol [42]. Specifically, a blocking tag impedes RFID scanning by simulating collisions in the singulation tree. Fig.5 depicts the framework of the above jamming or blocking-based protocols. Generally speaking, a blocker tag or a privacy enhanced device is used to actively broadcast a collision-bit mask when the legal or illegal readers are interrogating the tags. Then the legitimate reader further communicates with this device to recover the ID from the collision bits. Therefore, this device works as a proxy for the privacy-preserving interrogation.

Moreover, recently some researchers are using the signal spectral feature in physical layer to implement secure authentication in RFID systems. Kulseng et al. propose a lightweight solution to mutual authentication for RFID systems in which only the authenticated readers and tags can successfully communicate with each other [43]. Their protocols are realized utilizing minimalistic cryptography such as Physically Unclonable Functions (PUF) and Linear Feedback Shift Registers (LFSR), which are very efficient in hardware and particularly suitable for the low-cost RFID tags. By utilizing the dynamic bit encoding in the physical layer, Sakai et al. propose two novel RFID backward channel protection protocols for privacy protection against correlation attacks in RFID backward channel [44]. By leveraging the physical layer features, these protocols are able to greatly reduce the compute complexities in privacy protection and authentication.

B. Symmetric-key Encryption-based Solutions

1) Symmetric-key Encryption: The public key encryption is a powerful technique which can effectively implement the encryption and electronic signature. However, due to its complex operations, the public key encryption cannot be implemented in the RFID system, since the resource in the RFID tag is too few to support it. Therefore, the RFID system usually leverages the symmetric-key encryption to implement the security and privacy protection, as it has a much simpler processing logic. Specifically, the symmetric-key encryption can be used to authenticate the tags. Algorithm 1 depicts the protocol of authenticating the tags with the symmetric-key encryption [45]. In this protocol, any tag shares a distinct symmetric-key with the RFID reader.

Algorithm 1 Authenticate the tags with the symmetric-key encryption

1: The tag transmits the identifier T_i to the reader to identify itself.
2: The reader generates a random bit string R and transmits it to the tag.
3: The tag encrypts the bit string R with its key k_i, i.e.,$C = E_{ki}[R]$, and transmits C to the reader.
4: The reader locally computes $C' = E_{ki}[R]$, and verifies if $C' = C$. If yes, then the tag is authenticated.

Although the above protocol can authenticate the tags, it cannot effectively protect the privacy of the tag. As in step 1 the tag needs to transmit the identifier T_i to the reader, all adjacent RFID readers can overhear this message, which completely exposes the privacy of the tag. On the other hand, if the tag does not transmit the identifier T_i to the reader, then the reader cannot quickly find the corresponding key k_i to support the following operations. In order to protect the privacy during the authentication, in fact there exists a straightforward solution with poor performance: In comparison to Algorithm 1, the first step is omitted, the tag does not need to transmit the identifier T_i to the reader, instead it directly transmits the ciphertext $C = E_{ki}[R]$ according to the received bit string R. After receiving the ciphertext C, the reader locally enumerates all possible k_i to compute $C = E_{ki}[R]$, if there exists some key k_i to satisfy $C_i = C$, then the tag with the corresponding key is the one being authenticated. Assume that there are n tags in the search space, then the compute complexity of the search operation is $O(n)$. When the value of n is large, the time cost of the search operation is unacceptable. In order to address this problem, many researchers start to focus on how to fast search the data according to the received ciphertext. Song et al. propose practical techniques for searches on encrypted data [46]. Wang et al. propose private information retrieval techniques using trusted hardware [47, 48]. In order to fast search over the encrypted data, Chiu et al. maintain a monotonically increasing counter in the tag, and use it to conduct fast searching based on the binary splitting method [49].

2) Light-weight Solution: When the length of the key k_i is large enough (more than 128 bits), it is rather difficult to derive the key k_i within a short time simply according to the bit string

R and the ciphertext C. In this situation, the symmetric-key encryption-based protocols have high security. However, due to the limitation of manufacturing cost, the off-the-shelf RFID tags often have limited memory which is less than 512 bits, the number of logical gates is also very limited. In practical use of RFID systems, the length of bit string R, C and k_i is much less than the expected value to achieve the security standard. For example, Texas Instruments Inc. has devised the encrypted RFID tags used for vehicle security alarm systems. In consideration of the tag cost, the length of the bit string R and the key k_i is only 40 bits, the length of tag response C is only 24 bits. In this situation, techniques like the reverse engineering and password cracking can be used to crack the encryption systems. In order to address the above problem, the researchers have proposed various kinds of lightweight solutions to guarantee security. DESL [50] is a lightweight extension based on the traditional encryption protocol DES. It is specially devised to accommodate the resource requirement for those tiny computing devices like the RFID tags. HIGHT [51] is a protocol based on block encryption algorithm, which utilizes the 64-bit block and 128-bit key. The subkeys are generated during the process of encryption and decryption, which has a low requirement for the hardware resources. Realizing that most lightweight protocols are not fully conforming to the Gen2 standard, Sun et al. propose a novel authentication protocol based on Gen2, called Gen2+, for low-cost RFID tags. Gen2+ is a multiple round protocol using shared pseudonyms and Cyclic Redundancy Check (CRC) to achieve reader-to-tag authentication. Their protocol follows every message flow in Gen2 to provide backward compatibility [52].

3) Efficient Key Management: Recently a number of researchers have turned their attention to the privacy-preserving authentication in RFID systems. The key technical issue is how can a reader and tag that share a secret efficiently authenticate each other without revealing their identities to an adversary [53]. In order to tackle the above problem, an essential method is to implement the efficient key management in RFID systems. Based on how keys are managed in the system, the privacy preserving tag authentications proposed in the past can be mainly categorized into tree-based and group-based approaches.

The tree-based approaches employ tree structures to achieve fast authentication, which allow any pair of tags to share a number of key components. Dimitriou propose a lightweight protocol to the RFID privacy problem, which has the potential to guarantee user privacy without requiring changes to existing infrastructure or reducing business value from the use of RFID technology [54]. Lu et al. propose a strong and lightweight RFID private authentication protocol, SPA [55]. By designing a novel key updating method, they achieve the forward secrecy in SPA with an efficient key search algorithm. To address the heavy computational demand for the tree-based authentication, Li et al. design two privacy-preserving protocols based on cryptographical encoding [56], which significantly reduces both authentication data transmitted by each tag and computation overhead incurred at the reader. To address compromising attacks in the tree-based key management structure, Lu et al. propose an anti-compromising authentication protocol [57], which employs a novel sparse tree architecture, such that the key of every tag is independent from one another.

The group-based approaches are another novel authentication schemes which improves the tradeoff between scalability and privacy by dividing the tags into a number of tags. Hoque et al. propose a group-based anonymous private authentication protocol, which provides unlinkability and thereby preserves privacy [58]. The adversary cannot link the responses with the tags in the protocol, even if he/she can learn the identifier that the tags are using to produce the response. Based on the group-based method, Gong et al. design a fine-grained batch authentication scheme [59], which provides authentication results with accurate estimates of the number of counterfeiting tags and genuine tags.

While a tree-based approach achieves high performance in key authentication, it suffers from the issue of low privacy should a fraction of tags be compromised. On the contrary, while group-based key authentication is relatively invulnerable to compromise attacks, it is not scalable to the large number of tags. Therefore, recently several new techniques are proposed for private authentication based on various structures. Sakai et al. propose a new private tag authentication protocol based on skip lists [60]. Without sacrificing the authentication performance, their scheme provides a strong privacy preserving mechanism. In order to achieve forward secrecy and resistance to attacks, Yao et al. propose a lightweight RFID private authentication protocol based on the random walk concept [61].

C. Hash Function-based Solutions

In comparison to the symmetric-key encryption, in most cases an equivalent security mechanism can be implemented using the hash functions, but the implementation logic can be greatly simplified. Therefore, in recent years many researchers have focused on implementing a lightweight security mechanism using the hash function-based solutions. In regard to the RFID systems, although the implementation logic of hash function is fairly simple, it still exceeds the resource limitation of RFID tags. Therefore, the hash function in the RFID system should be further simplified. It is found that, the hash value can be derived from a pool of random bits pre-stored in the tag's onboard memory [33]. First, a string of 200 random bits can be generated for each tag by an offline random number generator, using the tag ID as the seed. The random bits are then stored in the tag. These bits form a logical ring. Then the hash function $H(ID, r)$ returns a certain number of bits after the rth bit in the ring. 200 random bits provide 200 different hash values, which are sufficient for general purpose usage.

The hash function-based protocols mainly include the hash-lock protocol, the randomized hash-lock protocol, and the hash chain protocol. Instead of using the real tag ID T_i, the hash-lock protocol [62] utilizes the $metaID$ (the hash value of the tag's key) for effective authentication to the RFID reader. In this way, the tag's ID can avoid being revealed. However, as the $metaID$ keeps unchanged for any tag, if the fixed $metaID$ is used in each response for a specified tag, then the RFID system is vulnerable to malicious tracking and replay attacks. The randomized hash-lock protocol [63] utilizes a

TABLE V
COMPARISON OF AUTHENTICATION AND PRIVACY PROTECTION SOLUTIONS

	Compute Complexity in Tag Side	**Scope of Applications**	**Resource Requirement**	**Flexibility**
Physical Mechanism-based Solutions	Very simple. The tag is not required to implement the logic for security and privacy protection.	Passive tags with very limited processing capacity.	Very few requirements, but additional devices are required to provide security and privacy protection.	Not flexible. The tag is either screened or fully exposed.
Symmetric-key Encryption-based Solutions	Complex. 20000-30000 logical gates are required.	Active tags or passive tags with higher processing capacity to conduct encryption and decryption.	High requirement. Enough processing and storage capability should be guaranteed.	Very flexible. Encryption and decryption can be effectively implemented.
Hash Function-based Solutions	Simple. A simple hash function can be easily implemented.	Passive tags to conduct authentication.	Few requirements. A hash function can be realized by 200 bit random series stored in the tag side.	Flexible. "Forward security" can be guaranteed, but encryption and decryption cannot be implemented.

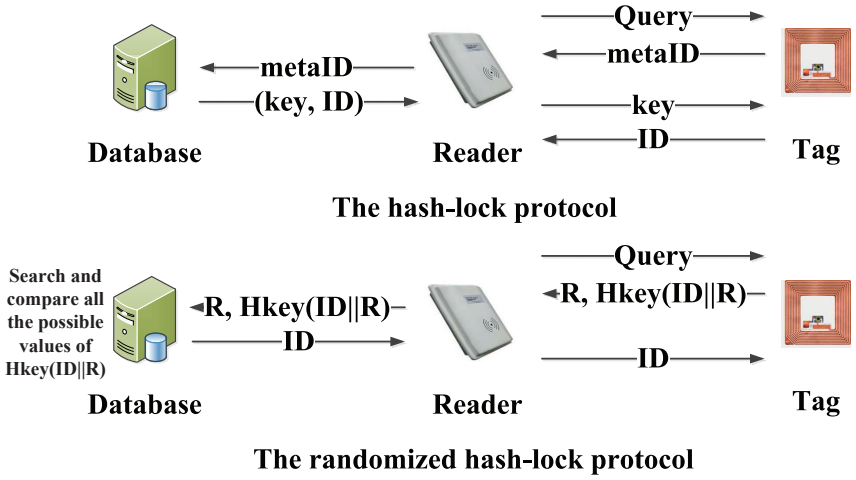


Fig. 6. The diagram of the hash-lock protocol and the randomized hash-lock protocol

random number-based inquiry and response mechanism. When the reader interrogates the tag, the tag first generates a random number R using the pseudo random number generator, then it computes the hash value $V = H_{key}(ID||R)$, finally it sends the hash value V and R to the reader. The reader conducts exhaustive search over the tags and computes all possible hash values $V' = H_{key}(ID||R)$ according to the tag ID. If $V' = V$ for a certain tag ID, then the reader successfully identifies the tag. The above mechanism can prevent the tag from replying a fixed message in each response, which can effectively avoid malicious tracking. But it cannot prevent the replay attacks, since the illegal user can overhear the random number R and the corresponding hash value V, and replay this message when the reader interrogates the tags, pretending to be the specified tag. Fig.6 provides the diagram of the hash-lock protocol and the randomized hash-lock protocol.

The hash-chain protocol [64] utilizes a shared secret-based inquiry and response mechanism. In this protocol, the reader and the tag share two hash functions G and H, as well as a random initial identifier s_1. When the reader interrogates a tag, the tag responds the current identifier $r_k = G(s_k)$ to the reader and locally updates $s_{k+1} = H(s_k)$. The reader searches the database with the identifier r_k to authenticates the tag, and updates s_k to synchronize with the tag. This mechanism leverages the "forward security" property of hash functions to update the tag response with each interrogation. In this way, the replay attack can be effectively avoided. However, the attacker can maliciously interrogate the tag multiple times, which breaks the synchronization between the reader and the tag. In this case, the authentication mechanism cannot work properly.

D. Comparative Study

In Table V, we compare and analyze the three kinds of solutions from four aspects: compute complexity, scope of applications, resource requirement and flexibility. Note that there are pros and cons for these three kinds of solutions. It is essential to choose a reasonable solution according to the specific application requirements and resource limitations.

E. Summing Up Challenges and Opportunities

According to the above recent research progress, we summarize the challenges and opportunities for authentication and privacy protection in Table VI, respectively for the physical mechanism-based solution, symmetric-key encryption-based solution, as well as Hash function-based solution.

TABLE VI
CHALLENGES AND OPPORTUNITIES FOR AUTHENTICATION AND PRIVACY PROTECTION

Mechanism	Challenges	Opportunities
Physical mechanism	Implementing in a recycled and delicate approach instead of brute-force approach.	The signal spectral feature in physical layer can be used to mitigate computing resource requirement.
Symmetric-key encryption	Complex operations and high requirement for computing resources.	Lightweight encryption and fast searching over encrypted data can be used to complement the protocols.
Hash function	Encryption and decryption cannot be effectively implemented.	Forward security can be cleverly leveraged for lightweight authentication.

V. LOCALIZATION AND ACTIVITY SENSING

In a number of RFID-based applications, the users conventionally have more demands than simply identifying the RFID tags. They require not only to "identify" the tags but also to "locate" the tags. The properties of the RFID tags like the received signal strength (RSS) have brought new opportunities to conduct accurate localization. For example, the backscattered signal strength has a significant reverse relationship with the distance between the reader and the tag. Generally speaking, as the distance increases, the backscattered signal strength is monotonically decreasing. Moreover, due to the far field propagation and the backscatter property, the signal strength is rather sensitive to the distance in the limited scanning range. Therefore, it is possible to measure the distance according to the backscattered signal and further estimate the location. By effectively leveraging the above information, the RFID system is able to accurately locate the objects.

Furthermore, it is noted that the backscattered signal strength is also very sensitive to the surrounding environment, i.e., the RSSI for a tag changes significantly when an object (e.g., a person) is passing by it. Therefore, a tag-free RFID-based activity sensing is inspired from the above phenomenon. In this section, we respectively introduce the research progress in localization and activity sensing based on RFID technology.

A. Accurate Localization

In regard to the localization, there are three key performance indicators as follows:

- Accuracy: the object should be accurately located to satisfy the demand for context-aware or location-based services in pervasive applications, i.e., the estimation error for localization should be made as small as possible.
- Time-efficiency: if the object is continuously moving, it is crucially important to locate the object in a real-time approach, i.e., the localization should be executed within specified time delay.
- Cost: the localization conventionally requires some precision instruments to measure the critical parameters, therefore, a cost-effective localization system is usually more preferred.

Besides, there are a number of performance indicators for the localization, including the fault tolerance, energy-efficiency, etc. The importance of these indicators depends on the particular application requirements.

Generally speaking, RFID-based localization can be classified into tag localization and reader localization. In the tag localization, each object to be located is attached with an RFID tag and one or more RFID readers are deployed in the environment. A server gathers data from the readers, executes a localization algorithm and notifies the result to the object. In the reader localization, the object carries an RFID reader and a set of RFID tags are deployed in the environment. The object uses the reader to actively obtain its own location. In the following, we respectively introduce the principles and related work in the tag localization and reader localization.

B. Locate the Tags

In regard to the tag localization, the tag is usually located according to the Received Signal Strength Indicator (RSSI). A straightforward approach to use RSSI is building a model to depict the mapping relationship between the RSSI and the distance. In this way, the actual distance between the tag and the reader can be measured by the received signal strength in the reader. Moreover, the measured distances from an unknown tag to several RFID readers constrain the presence of this tag. The exact location of this tag can be effectively estimated by using the method of trilateration or multilateration. Therefore, for the distance-based positioning, the most important thing is how to measure distances in the physical world. In theory, radio signal strengths diminish with distance according to a power law. A generally employed model for wireless radio propagation is proposed in [65]. However, the radio propagation in RFID systems is severely impacted by the issues like ambient noises, path loss and multi-path effect, which makes the above model rather unreliable. How to eliminate such effect so as to enhance the indoor localization performance is a big challenge. Many ranging techniques are proposed and developed in RFID systems. Hightower et al. present SpotON [66], a new tagging technology for 3D localization based on radio signal strength analysis. They propose an aggregation algorithm to minimize signal strength error relative to empirical data. After mapping the signal strength measurements to an approximate distance, they aggregate the values to triangulate the precise position of the tagged object. Most existing indoor positioning systems can't adapt to the environmental variations well, as they need an accurate signal propagation model. Xiao et al. propose an environmental-adaptive RSSI-based indoor positioning approach using RFID [67], in which the parameters of signal propagation model are updated online in a closed-loop feedback correction manner. Brchan et al. propose a real-time localization system [68], using efficient multiple propagation models to compensate for the drawback of the received signal strength technique.

Another approach to use RSSI is collecting the fingerprints of the measured RSSI at each location of the positioning area. Suppose multiple readers are deployed in the positioning area, when a tag is deployed at the labeled location, the RSSI fingerprint can be collected by measuring the received signal strength at each reader. In this way, the RSSI fingerprint is recorded as a vector, with its size equal to the number

of readers. This process is known as site survey. Then, in regard to the target tag at an unknown location, the measured RSSI is matched with recorded fingerprints. The location of the most similar fingerprint is returned as the location of the target object. The idea of RSSI fingerprint is nowadays widely used in wireless indoor localization. Realizing the site survey involves intensive costs on manpower and time, Yang et al. investigate novel sensors integrated in modern mobile phones and leverage user motions to construct the radio map of a floor plan [69], which is previously obtained only by site survey. Similarly, Rai et al. present a system that makes the site survey zero-effort, by enabling RSSI fingerprint to be crowdsourced without any explicit effort on the part of users [70]. In regard to RFID systems, Deyle et al. propose a new mode of perception that produces images of the spatial distribution of RSSI for each of the tagged objects in the positioning area [71]. The intensity of each pixel in the "RSSI image" is the measured RF signal strength for a particular tag in the corresponding position.

In order to further improve the overall accuracy of locating objects, the concept of reference tags is proposed. LANDMARC [72] is one of the first research work to locate the RFID tag based on the reference tags. It employs the idea of having extra fixed location reference tags to support location calibration. These reference tags serve as reference points in the system. When locating a target tag, the readers simultaneously interrogate the target tag and the reference tags, and get the RSSI from these tags. Then, by comparing different RSSI values of the reference tags with the target tag, the target tag can be located from the nearest neighboring reference tags in terms of RSSI value. In this way, the environmental dynamics can easily be accommodated. Their approach helps offset many environmental factors that contribute to the variations in scanning range, because the reference tags are subject to the same effect in the environment as the tags to be located. However, LANDMARC suffers from two drawbacks. First, it does not work well in a closed area with severe radio signal multi-path effects. Second, to further improve the localization accuracy, more reference tags are needed which is costly and may trigger the RF interference phenomenon. Based on this understanding, the VIRE system [73] is further proposed to overcome the above drawbacks without additional cost. They leverage the concept of virtual reference tags to maintain a proximity map for each reader. An elimination algorithm is used to eliminate those unlikely locations to reduce the estimation error. Realizing that the reference tags may introduce some side-effect like providing some unreasonable signal strength, Nick et al. propose to use unscented Kalman filter to help reduce the localization errors [74]. Khan et al. make an attempt to extend the LANDMARC algorithm by introducing the "z" coordinate [75]. They utilize the passive tag instead of active tag, which essentially cuts the cost of localization system drastically. Chen et al. design an adaptive, accurate indoor localization scheme using passive RFID systems, i.e., the adaptive power stepping and the adaptive calibration, which can adaptively adjust the critical parameters and leverage the feedbacks to improve the localization accuracy. The realistic experiment results indicate that they can achieve an accuracy of 31 cm within 2.6 seconds on average [76]. Fig.7 shows an example of the reference tag-based localization, the reference tags are deployed in known positions, the target tags are located according to the nearest neighbors in terms of RSSI. The readers are usually deployed on the boundary of the location area to interrogate these tags.

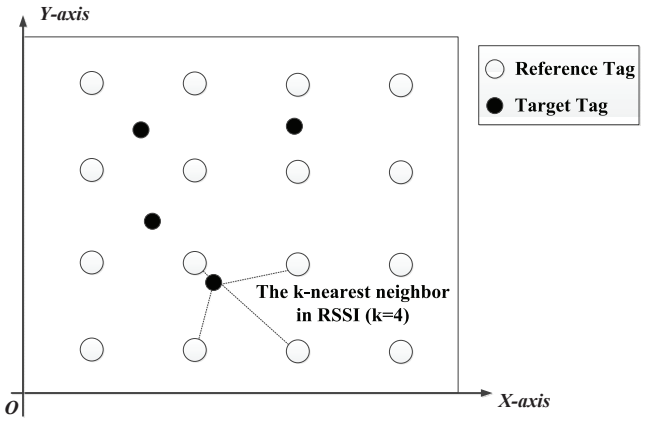


Fig. 7. An example of the reference tag-based localization

Besides using the RSSI as the measurement for localization, recently a number of researchers attempt to use the phase of the received signal as a measurement to execute the localization. Nikitin et al. propose three main techniques based on PDOA (Phase Difference of Arrival) [77]: TD (Time Domain), FD (Frequency Domain), and SD (Spatial Domain). Miesen et al. present a localization method based on phase values sampled from a synthetic aperture by a RFID reader [78]. The calculated result is a spatial probability density function that reveals the actual RFID tag position. Wille et al. propose a phase difference based RFID navigation for medical applications [79]. They applied a machine learning algorithm to phase difference data gathered from multiple RFID receivers. In addition to this, the Angle of Arrival (AOA) mechanisms are also explored for accurate localization in RFID systems. Azzouzi et al. present new measurement results for an Angle of Arrival (AoA) approach to localize RFID tags [80]. The AoA is estimated using the phase differences in the complex baseband signals of adjacent antenna elements within one array. Wang et al. consider direction-of-arrival estimation techniques for application to near-field narrowband RFID problems [81]. They examine the use of a pair of RFID antennas to track moving RFID tagged items through a portal, which yields a simple way for identifying the direction of the tag movement.

C. Locate the Readers

In reader localization, an object carrying an RFID reader is located by communicating with some RFID tags deployed in the environment. Specifically, the tags generally work as the anchor nodes with accurate positions in the deployment area, the reader is then located according to the backscattered signal from the scanned tags. Compared with tag localization, reader localization reduces infrastructure cost by using cheap tags instead of expensive readers. Realizing that frequent occurred

TABLE VII
COMPARATIVE STUDY OF THE LOCALIZATION SOLUTIONS

	Accuracy	Time-efficiency	Deployment Cost	Hardware Cost
Range-based localization using RSSI (RL)	Low	High	Low	Low
RSSI fingerprint-based localization (FL)	High	High	High	Low
Reference tag-based localization using RSSI (RTL)	Median	Low	Median	Low
Phase-based localization (PL)	High	Median	Low	High
Angle of Arrival based localization (AAL)	High	Median	Low	High

RFID faults greatly affect the localization accuracy, in order to tackle this problem, Zhu et al. propose an effective fault-tolerant RFID reader localization approach suitable for the above situations, and illustrate how to measure the quality of a localization result [82]. In order to deal with the noisy RFID readings gathered in object tracking applications, Yang et al. propose a hybrid method for tracking mobile objects with high accuracy and low computational cost [83], such that the computational cost of filtering the noises can be greatly reduced.

D. Activity Sensing

Activity sensing has drawn many attentions in recent years, and it has yielded lots of research results. Most of them are related to vision-based schemes and surveillance technologies. The surveillance technologies are further classified into the Bluetooth, infrared, ultrasonic and sensor based solutions. These solutions mainly require fairly expensive equipments to capture scenarios as video or other sensor data, moreover, a lot of energy is expended for these equipments during the procedure of activity sensing. These issues greatly limit the range of applications, as most pervasive applications cannot afford such a huge overhead in terms of both deployment cost and energy consumption.

Therefore, a low-cost, low-power technology is desperately required for activity sensing. Technological advances in RFID has provided the opportunities for activity sensing in an economically attractive approach. By exploiting the phenomenon that RSSI changes significantly when an object is passing by, Liu et al. propose to use RFID tag arrays for activity sensing in a device-free approach, i.e., the tracking objects do not need to attach any transmitters or receivers, such as tags or readers [84]. By developing a practical fault-tolerant method, they offset the noise of RF tag data and mine frequent trajectory patterns as models of regular activities. Zhang et al. further propose TASA, a tag-free activity sensing using RFID tag arrays for location sensing and route tracking [85]. Being different from the previous scheme [84], TASA uses passive tag arrays together with a few active reference tags, instead of all active tags. Moreover, by reducing noise in the readings of passive RFID tags, TASA is much effective for locating multiple moving objects.

E. Analysis

In order to get a better understanding of the features for the aforementioned localization schemes, we compare their performance in terms of accuracy, time-efficiency, deployment cost and hardware cost. Here, the accuracy denotes the precision of localization, the time-efficiency denotes the locating speed, the deployment cost denotes the human cost of deploying the localization system and getting the training data, the hardware cost denotes the fixed cost of the RFID readers and tags in the localization systems.

Table VII depicts the performance comparison of the localization solutions. In order to make it clear and concise, in the following we respectively use the abbreviations RL, FL, RTL, PL and AAL to denote the corresponding location schemes. In regard to the accuracy, FL, PL and AAL all achieve high accuracy in localization, the localization errors can conventionally be limited to at most 0.5m. RTL achieves a median accuracy by limiting the errors to at most 1m. RL achieves a low accuracy with the localization errors of at most 5m. In regard to the time-efficiency, both RL and FL achieve high-efficiency since they only require to obtain the RSSI from the target tag. PL and AAL achieve median-efficiency as more refined data are required and more computations are involved in the localization. RTL achieves low-efficiency in time, because the RSSIs from multiple tags are required to be obtained, which can be very time consuming. In regard to the deployment cost, RL, PL and AAL have a low cost as only the RFID readers are required to be deployed. RTL has a median deployment cost since the reference tags are necessarily to be deployed in advance. FL has a high deployment cost as collecting the training data of RSSI fingerprints is rather time-consuming and inconvenient. In regard to the hardware cost, RL, FL and RTL have a low cost in hardware as conventional off-the-shelf RFID readers can effectively collect the RSSI for localization. PL and AAL introduce a high cost since they require precise instrument to obtain the measurements like the phase and angle of signals.

F. Summing Up Challenges and Opportunities

According to the above recent research progress, we summarize the challenges and opportunities for RFID localization and activity sensing in Table VIII. We believe that, by sufficiently exploring the underlying opportunities in localization and activity sensing, the challenges can be gradually overcome to finally achieve accurate and real-time perception of locations and activities.

TABLE VIII
CHALLENGES AND OPPORTUNITIES FOR RFID LOCALIZATION AND ACTIVITY SENSING

Mechanism	Challenges	Opportunities
RFID localization	The unstable communication in the backscatter channel makes accurate localization hard to achieve.	The low cost and battery-free property make large scale deployment of reference tags possible. The sensitivity to ambient environment contributes to accurately depict the differences among various positions.
Activity sensing	Complex activities cannot be accurately perceived in a real-time approach due to the limited perception in RFID systems.	It is possible to implement device-free activity sensing by exploring the sensitivity to the surrounding mobile environment in RFID system.

VI. PERFORMANCE TUNING IN REALISTIC SETTINGS

As a new emerging technology, RFID has been widely explored from various aspects by a lot of researchers in recent years. However, most former research work mainly consider optimized design of algorithms and protocols under a relatively ideal transmission environment, and evaluate the performance through simulations. As a matter of fact, a number of physical factors in realistic transmission environment, like path loss, energy absorption and signal interference, have brought great unreliability to normal operations in RFID systems. Therefore, it is essential to consider the performance tuning in realistic settings, such that the performance of algorithms and protocols can be guaranteed for realistic applications.

A. Critical Factors for System Performance

In realistic settings, a lot of factors can impact the performance of RFID systems, in the following we elaborate those critical factors which are closely correlated with the system performance.

The reader's power: If the reader's power is too small, then the effective scanning range is reduced. In this situation, some tags cannot be activated as the incident power is below the activation threshold, or the reader cannot successfully resolve the backscattered signal as the backscattered signal noise ratio is rather low. If the reader's power is too large, then the effective scanning range is increased. In this situation, the backscattered signal strength of some tags is greatly increased, amplifying the signal interference among tags.

The path loss, multi-path effect, and energy absorption: All the three issues can lead to the signal attenuation in RFID systems, which greatly impacts both the forward link transmission (from the reader to tag) and reverse link transmission (from the tag to reader).

The signal interference: As multiple readers are conventionally deployed in RFID applications, there exist three kinds of interference in RFID systems: (1) tag-tag interference: multiple tags respond to the reader simultaneously and cause collisions at the reader, (2) reader-tag interference: response from the tag to a reader is "drowned" by the signal from another reader, (3) reader-reader interference: signal from multiple readers collide at a tag. The above interference can cause bit errors during data transmission, thus reducing the reading efficiency of RFID systems.

The deployment of tags: If the tags are densely deployed, the incident power from the reader can be fully diluted among the tags, and the signal interference and energy absorption can be aggravated among the tags. For a specified tag, if the incident angle of the power parallels the tag's plane (also known as the tag antenna's plane), then it is impossible for the tag to backscatter a strong enough signal. Hence, the incident power should be perpendicular to the tag's plane as much as possible. Table IX illustrates the impact of these critical factors on the system performance metrics, including the scanning range, read throughput and energy consumption.

B. Experimental Findings

Since the above factors are ubiquitous in the realistic settings, it is very difficult to achieve good performance according to the algorithms and optimized parameters derived from ideal settings. Therefore, in recent years a lot of researchers have paid attention to the performance tuning for RFID systems in realistic settings. In order to depict the impact of communication error on the anti-collision performance of Gen2 RFID system, Kawakita et al. provide experiment results to prove that the bit errors in physical layer greatly reduce the overall performance [86]. Buettner et al. examine the performance of EPC Class-1 Gen-2 UHF RFID systems in realistic settings, and identify factors that degrade overall performance and reliability with a focus on the physical layer [87]. They find that physical layer considerations have a significant impact on reader performance, and that this is exacerbated by a lack of integration between the physical and MAC layers. Aroor el al. use a simple, empirical, experimental approach to evaluate the performance of the commercially available RFID systems [88]. By varying the reading distance between the reader and the tags, they examine various performance parameters in various environments (including free space, near-water and near-metal environment). Ramakrishnan et al. provide comprehensive performance benchmarks for passive UHF RFID systems [89], which can effectively depict the reading efficiency of RFID systems in realistic settings. Jeffery et al. conduct experiments in realistic settings and find that within each reader's detection range, a large difference exists in reading performance [90]. Specifically, within each readers detection range, there are two distinct regions: the major detection region and the minor detection region. The major detection region is the area directly in front of the reader, giving high detection probability, and the minor detection region extends from the end of the major detection region to the edge of the detection range, where the read ratio drops off to zero at the end of the detection range. Xie et al. show the first comprehensive experimental study on mobile RFID reading performance based on a relatively large number of tags [23]. By making a number of observations regarding the tag reading performance, they have a few important new findings from the experiments. For example, the probabilistic backscattering is a ubiquitous phenomenon of the RFID system in realistic settings, which has an important effect on the reading performance. Besides, it is not wise to blindly increase the readers power for tag identification, which can degrade the overall performance including the effective throughput and energy consumption.

TABLE IX
CRITICAL FACTORS FOR SYSTEM PERFORMANCE

	Scanning Range	Read Throughput	Energy Consumption
Reader's power	The effective scanning range increases/decreases as the power is increased/decreased.	If the power is too small, some tags cannot be effectively activated or identified; If the power is too large, the interferences among tags are increased, thus the throughput is reduced.	The energy consumption increases/decreases as the power is increased/decreased.
Path loss, multi-path effect, energy absorption	Signal attenuation is caused, thus the effective scanning range is reduced.	Some tags in the normal scanning range cannot be effectively activated or identified, the throughput is reduced.	The reader has to increase the power to compensate the energy loss in signal propagation, the energy consumption is increased.
Signal interference	The backscattered signals of some tags cannot be effectively resolved due to the interference, the effective scanning range is reduced.	The probability of bit errors in transmitting is increased, the throughput is reduced.	The reader needs to reasonably adjust the power to prevent too many interferences, which will change the energy consumption.
Deployment of tags	Dense deployment of tags will affect the electromagnetic field of the reader's antennas, and change the reader's effective scanning range.	If the tag's plane is perpendicular to the incident power, the backscatter efficiency is improved, then the read throughput is increased.	Unreasonable deployment of tags causes the reader to increase the power to enhance the backscattered signal strength, thus the energy consumption is increased.

Realizing that the reader's transmission power actually has a significant impact on the reading performance of the RFID system, a number of researchers start to investigate into this area. Xu et al. investigate the impact of transmission power on reading performance through extensive empirical study on passive tags [91][92]. While exploring the relationship between the transmission power and the response quality, they reveal that there exists a "lossy state" of passive tags where the reader cannot detect tags due to insufficient power although tags could have responded. Based on this understanding, they present an energy-efficient inventory algorithm. It incrementally adjusts power level to use sufficient but not excessive power for tag identification. Su et al. find that, when the transmission power is set to a reasonable range, the "capture effect" can be used to resolve the collision slots into singleton slots [93]. More specifically, the "capture effect" helps tags near the reader to transmit their data although collision had occurred in the time slot they used, since their signal is stronger than the farthest tags due to channel attenuation. Therefore, they propose a progressing scanning algorithm to improve the reading throughput.

Generally speaking, empirical and experimental studies in this area are relatively few. In order to guarantee the reading performance of RFID systems in real applications, the performance tuning of RFID systems in realistic settings should get continuous attention from researchers in academia and industry.

VII. FUTURE RESEARCH DIRECTIONS

Although the study and research of RFID technology has already get much achievement, there are still a lot of challenging problems yet to be solved. In order to help researchers to get a better grasp of future research directions in the area of RFID, we provide more insights into the future research challenges and opportunities as follows:

(1) *Carrying out cross-layer optimization in RFID data management*: The idea of "cross-layer optimization" originates from the protocol design of wireless network. The core idea is to realize the optimized control and information exchange among two or more protocol layers, such that the performance of network systems can be greatly improved. In the research area of sensor network, the idea of cross-layer optimization has been widely accepted and used. However, previously only a few researchers leveraged this idea to solve the problems in RFID systems [94] [95]. We find that it is usually rather difficult to solve a certain problem, e.g., privacy protection and authentication in RFID system, from a single layer's view. However, given the cross-layer information, these problems can be skillfully solved by extracting and integrating the features from various layers. For example, by correlating the signal spectral features in the physical layer and the usage pattern detected in the application layer, the specified tags can be effectively authenticated in RFID systems. Therefore, on the one hand, if we do not sufficiently consider the influence among different layers, the corresponding research results cannot achieve the expected performance in realistic applications; on the other hand, the resource scarcity of the RFID system proposes the pressing needs to devise lightweight protocols and algorithms, the cross-layer optimization provides opportunities to solve the traditional problems from a different aspect, by tactfully leveraging the features from different layers.

(2) *Breaking through the traditional thinking to realize RFID security and privacy protection*. Note that it it rather difficult to rely on traditional security mechanisms to guarantee the security and privacy of RFID systems. The great challenge is brought by the resource scarcity of the RFID tags, which is vulnerable to outside interferences and can only afford limited computation. Therefore, it is essential to break through the traditional thinking to realize a set of novel security schemes for RFID systems. Fortunately, it is noted that some special physical properties can be leveraged to implement the corresponding security schemes. For example, the backscatter-based communication brings the "proximity effect", i.e., only those tags in the vicinity of the RFID reader can be interrogated in a real-time approach. Besides, the signal fingerprints in the physical layer can be used to construct the "physical one-way function" to implement the properties like the hash function. Therefore, how to leverage

the aforementioned physical properties to devise novel security schemes for RFID system is a challenging and promising research problem.

(3) *Developing application-driven localization and activity sensing using active/passive RFID systems*: Due to the widespread applications of context-aware and location-based services, the localization in RFID systems is basically application-driven. For future research in localization, besides the metrics of accuracy and time-efficiency, more properties are expected to be satisfied, such as the fault tolerance and cost-efficiency. Here, the fault tolerance requires the localization scheme to effectively deal with outliers and be robust to the noisy readings. The cost-efficiency requires the localization scheme to sufficiently reduce all kinds of cost including the hardware cost, computation cost, energy cost and labor cost. In fact, it is up to the specific application to decide which properties are essential to be obtained. In essence, obtaining a Pareto improvement is a major challenge. That is, increasing the performance of one of the metrics without degradation on others.

(4) *Developing software-defined RFID readers for more-refined performance tuning*: It is known that the system performance is impacted by issues from various protocol layers, e.g., the frame size of each query round, the coding scheme and bit rate for transmission, and so on. However, it is rather difficult to understand how these issues interactively and integrally affect the performance metrics in realistic settings. Due to various reasons, current off-the-shelf RFID readers do not support to access or set these underlying parameters and feedbacks for performance improvement. Besides, a single reader can only support a typical protocol standard, without being compatible with the other kinds of standards. Therefore, it is neither convenient nor cost-effective for researchers to investigate the RFID system through the commercial readers. The software-defined radios (SDR) have provided opportunities for more-refined performance tuning in a cost-effective approach. If the software-defined RFID reader can be effectively developed, the users can deliberately set those critical parameters and obtain the underlying feedbacks for performance tuning. Moreover, it is ready to support a new form of RFID communication protocol simply by running new software on existing SDR hardware.

(5) *Exploring novel application modes for RFID systems*: The original design purpose of RFID systems is to efficiently label and identify the items, the current applications of RFID systems still remain in the areas like supply chains: tracking, managing and monitoring the goods. In recent years, RFID has been widely used in various kinds of applications with its unique advantage, e.g., anti-counterfeiting, anti-theft, the food and drug safety, etc. In fact, whether the RFID technology can be spread to new applications depends on whether feasible application patterns can be fully exploited according to RFID's unique features. Exploration into application patterns of RFID mainly includes two aspects: 1) replacing the current application patterns with RFID in a low-cost approach and 2) explore novel application patterns for RFID. For example, besides identifying the items, the RFID tag itself is a tiny wireless device, its properties like the signal strength and coding scheme have provided technical support for application patterns like localization, tracking and authentication. The user memory of RFID tags can support more than 512-bit storage, conventionally it can store over 32 English characters, more information can be further stored with the index number. This provides effective support for intelligent applications based on information retrieval and query.

VIII. Conclusion

As a key technology of automatic identification, RFID has attracted increasing attention in recent years. In this article, we have discussed several research challenges and opportunities, and provided an overview of existing solutions, including anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings. Focusing on RFID data management, we describe and analyze the research work on three aspects: algorithm, protocol and performance evaluation. We offer this survey to help researchers to understand the state-of-the-art research progress and to address directions of future research in the area of RFID.

References

[1] S. Shepard, *RFID : radio frequency identification*. McGraw-Hill Networking Professional, Aug. 2004.

[2] E. Ilie-Zudora, Z. Kemnya, F. van Blommesteinb, L. Monostoria, and A. van der Meulen, "A survey of applications and requirements of unique identification systems and rfid techniques," *Computers in Industry*, vol. 62, no. 3, p. 227C252, April 2011.

[3] P. M. Reyes, G. V. Frazier, E. L. Prater, and A. R. Cannon, "Rfid: the state of the union between promise and practice," *Int. J. of Integrated Supply Management*, vol. 3, no. 2, Jan. 2007.

[4] J. Wu, S. Rangan, and H. Zhang, *Green Communications: Theoretical Fundamentals, Algorithms and Applications*. CRC Press, Sept. 2012.

[5] E. Hossain, V. Bhargava, and G. P. Fettweis, *Green Radio Communication Networks*. Cambridge University Press, Aug. 2012.

[6] K. Finkenzeller and D. Mller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiley, Aug. 2010.

[7] H. Lehpamer, *RFID Design Principles*. Artech House Publishers, Feb. 2012.

[8] R. Weinstein, "Rfid: a technical overview and its application to the enterprise," *IT Professional*, vol. 7, no. 3, pp. 27 – 33, 2005.

[9] C. Turcu, *Current Trends and Challenges in RFID*. InTech, July 2011.

[10] D. Klair, K.-W. Chin, and R. Raad, "A survey and tutorial of rfid anti-collision protocols," *IEEE Commun. Surveys and Tutorials*, vol. 12, no. 3, Aug. 2010.

[11] J. Myung, W. Lee, and S. Jaideep, "Adaptive binary splitting for efficient rfid tag anti-collision," *IEEE Commun. Lett.*, vol. 10, no. 3, pp. 144–146, 2006.

[12] L. Pan and H. Wu, "Smart trend-traversal: A low delay and energy tag arbitration protocol for large rfid systems," in *Proc. 28th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2009.

[13] Y. Maguire and R. Pappu, "An optimal q-algorithm for the iso 18000-6c rfid protocol," *IEEE Trans. Automation Science and Engineering*, vol. 6, no. 1, pp. 16–24, 2009.

[14] B. Zhen, M. Kobayashi, and M. Shimuzu, "Framed aloha for multiple rfid objects identification," *IEICE Trans. Commun.*, vol. E88-B, no. 3, pp. 991–999, 2005.

[15] F. Schoute, "Dynamic frame length aloha," *IEEE Trans. Commun.*, vol. 31, no. 4, pp. 565–568, 1983.

[16] C. Floerkemeier, "Bayesian transmission strategy for framed aloha based rfid protocols," in *Proc. IEEE Int. Conf. on RFID*, 2007.

[17] H. Vogt, "Efficient object identification with passive rfid tags," in *Proc. 1st Int. Conf. on Pervasive Computing*, 2002.

[18] S. Lee, S. Joo, and C. Lee, "An enhanced dynamic framed slotted aloha algorithm for rfid tag identification," in *Proc. 2nd Annu. Int. Conf. on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous)*, 2005.

[19] S. Tang, J. Yuan, X. Y. Li, G. Chen, Y. Liu, and J. Zhao, "Raspberry: A stable reader activation scheduling protocol in multi-reader rfid systems," in *Proc. 17th IEEE Int. Conf. on Network Protocols*, 2009.

[20] L. Yang, J. Han, Y. Qi, C. Wang, T. Gu, and Y. Liu, "Season: Shelving interference and joint identification in large-scale rfid systems," in *Proc. 30th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2011.

[21] B. Sheng, L. Q, and M. W, "Efficient continuous scanning in rfid systems," in *Proc. 29th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2010.

[22] L. Xie, B. Sheng, C. C. Tan, H. Han, Q. Li, and D. Chen, "Efficient tag identification in mobile rfid systems," in *Proc. 29th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2010.

[23] L. Xie, Q. Li, X. Chen, S. Lu, and D. Chen, "Continuous scanning with mobile reader in rfid systems: An experimental study," in *Proc. 14th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2013.

[24] Y. Yin, L. Xie, J. Wu, A. V. Vasilakos, and S. Lu, "Focus and shoot: Efficient identification over rfid tags in the specified area," in *Proc. Int. Conf. on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, 2013.

[25] M. Kodialam and T. Nandagopal, "Fast and reliable estimation schemes in rfid systems," in *Proc. 12th Annu. Int. Conf. Mobile Computing and Netw. (MobiCom)*, 2006.

[26] W. Chen, "An accurate tag estimate method for improving the performance of an rfid anticollision algorithm based on dynamic frame length aloha," *IEEE Trans. Automation Science and Engineering*, vol. 6, no. 1, pp. 9–15, 2009.

[27] H. Han, B. Sheng, C. C. Tan, Q. Li, W. Mao, and S. Lu, "Counting rfid tags efficiently and anonymously," in *Proc. 29th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2010.

[28] Q. Chen, H. Ngan, Y. Liu, and L. Ni, "Cardinality estimation for large-scale rfid systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 9, pp. 1441–1454, 2011.

[29] Q. Chen, Y. Liu, H. Ngan, and L. Ni, "Asap: Scalable identification and counting for contactless rfid systems," in *Proc. 30th IEEE Int. Conf. on Distrib. Computing Syst. (ICDCS)*, 2010.

[30] M. Shahzad and A. X. Liu, "Every bit counts: fast and scalable rfid estimation," in *Proc. 18th Annu. Int. Conf. on Mobile Computing and Networking (MobiCom)*, 2012.

[31] B. Sheng, C. C. Tan, Q. Li, and W. Mao, "Finding popular categories for rfid tags," in *Proc. 9th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2008.

[32] M. Kodialam, T. Nandagopal, and W. Lau, "Anonymous tracking using rfid tags," in *Proc. 26th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2007.

[33] T. Li, S. Chen, and Y. Ling, "Identifying the missing tags in a large rfid system," in *Proc. 11th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2010.

[34] Y. Qiao, S. Chen, T. Li, and S. Chen, "Energy-efficient polling protocols in rfid systems," in *Proc. 12th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2011.

[35] S. Chen, M. Zhang, and B. Xiao, "Efficient information collection protocols for sensor- augmented rfid networks," in *Proc. 30th Annu. Joint Conf. of the IEEE Computer and Commun. Societies (INFOCOM)*, 2011.

[36] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free batch authentication for rfid tags," in *Proc. 18th IEEE Int. Conf. on Network Protocols (ICNP)*, 2010.

[37] Y. Zheng and M. Li, "Fast tag searching protocol for large-scale rfid systems," in *Proc. 19th IEEE Int. Conf. on Network Protocols (ICNP)*, 2011.

[38] S. E. Sarma, S. A. Weis, and D. W. Engels, "Rfid systems and security and privacy implications," in *Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2002.

[39] S. Inoue and H. Yasuura, "Rfid privacy using user-controllable uniqueness," in *Proc. RFID Privacy workshop*, 2003.

[40] J. D. Krauss, *Electromagnetics, 4Ed*. McGraw-Hill, 1992.

[41] T. Lim, T. Li, and S. Yeo, "A cross-layer framework for privacy enhancement in rfid systems," *Pervasive and Mobile Computing*, vol. 4, no. 6, pp. 889–905, 2008.

[42] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of rfid tags for consumer privacy," in *Proc. 10th ACM Conf. on Computer and Commun. Security (CCS)*, 2003.

[43] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for rfid systems," in *Proc. IEEE INFOCOM*, 2010.

[44] K. Sakai, W. Ku, R. Zimmermann, and M. Sun, "Dynamic bit encoding for privacy protection against correlation attacks in rfid backward channel," *IEEE Trans. Comput.*, vol. 62, no. 1, pp. 112–123, 2013.

[45] A. Juels, "Rfid security and privacy: a research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, 2006.

[46] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symp. on Security and Privacy*, 2000.

[47] S. Wang, X. Ding, R. H. Deng, and F. Bao, "Private information retrieval using trusted hardware," in *Proc. 11th European Symp. on Research in Computer Security (ESORICS)*, 2006.

[48] Z. Yang, S. Zhong, and R. N. Wright, "Privacy-preserving queries on encrypted data," in *Proc. 11th European Symp. on Research in Computer Security (ESORICS)*, 2006.

[49] C. C. Tan, Q. Li, and L. Xie, "Privacy protection for rfid-based tracking systems," in *Proc. IEEE Int. Conf. on RFID*, 2010.

[50] A. Poschmann, G. Leander, K. Schramm, and C. Paar, "New lightweight crypto algorithms for rfid," in *Proc. IEEE Int. Symp. on Circuits and Systems (ISCAS)*, 2007.

[51] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, H. Kim, and S. Chee, "Hight: A new block cipher suitable for low-resource device," in *Proc. 8th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2006.

[52] H. Sun and W. Ting, "A gen2-based rfid authentication protocol for security and privacy," *IEEE Trans. Mobile Comput.*, vol. 8, no. 8, pp. 1052–1062, 2009.

[53] D. Molnar and D. Wagner, "Privacy and security in library rfid issues, practices, and architectures," in *Proc. 11th ACM conf. on Computer and commun. security (CCS)*, 2004.

[54] T. Dimitriou, "A secure and efficient rfid protocol that could make big brother (partially) obsolete," in *Proc. IEEE Int.l Conf. on Pervasive Computing and Commun. (PerCom)*, 2006.

[55] L. Lu, J. Han, L. Hu, Y. Liu, and L. Ni, "Dynamic key-updating: Privacy-preserving authentication for rfid systems," in *Proc. IEEE Int. Conf. on Pervasive Computing and Commun. (PerCom)*, 2007.

[56] T. Li, W. Luo, Z. Mo, and S. Chen, "Privacy-preserving rfid authentication based on cryptographical encoding," in *Proc. IEEE INFOCOM*, 2012.

[57] L. Lu, J. Han, R. Xiao, and Y. Liu, "Action: Breaking the privacy barrier for rfid systems," in *Proc. IEEE INFOCOM*, 2009.

[58] M. Hoque, F. Rahman, and S. Ahamed, "Anonpri: An efficient anonymous private authentication protocol," in *Proc. IEEE Int. Conf. Pervasive Computing and Commun. (PerCom)*, 2011.

[59] W. Gong, K. Liu, X. Miao, Q. Ma, Z. Yang, and Y. Liu, "Informative counting: Fine-grained batch authentication for large-scale rfid systems," in *Proc. 14th ACM Int. Symp. on Mobile ad hoc networking and computing (MobiHoc)*, 2013.

[60] K. Sakai, M. Sun, W. Ku, and T. Lai, "Randomized skip lists-based private authentication for large-scale rfid systems," in *Proc. 14th ACM Int. Symp. on Mobile ad hoc networking and computing (MobiHoc)*, 2013.

[61] Q. Yao, Y. Qi, J. Han, J. Zhao, X. Li, and Y. Liu, "Randomizing rfid private authentication," in *Proc. IEEE Int. Conf. Pervasive Computing and Commun. (PerCom)*, 2009.

[62] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio frequency identification: Secure risks and challenges," *RSA Laboratories Cryptobytes*, vol. 6, no. 1, pp. 2–9, 2003.

[63] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspect s of low-cost radio frequency identification systems," in *Proc. 1st Int. Conf. on Security in Pervasive Computing (SPC)*, 2003.

[64] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash chain based forward secure privacy protection scheme for low cost rfid," in *Proc. Symp. on Cryptography and Information Security (SCIS)*, 2004.

[65] S. Y. Seidel and T. S. Rappaport, "914mhz path loss prediction models for indoor wireless communications in multifloored buildings," *IEEE Trans. Antennas Propag.*, vol. 40, no. 2, pp. 209–217, 1992.

[66] J. Hightower, G. Borriello, and R. Want, "Spoton: An indoor 3d location sensing technology based on rf signal strength," Univ. Washington, Tech. Rep., 2000.

[67] X. Xiao, X. Jing, S. You, and J. Zeng, "An environmental-adaptive rssi based indoor positioning approach using rfid," in *Proc. Int. Conf. on Advanced Intelligence and Awarenss Internet*, 2010, pp. 127–130.

[68] J. Brchan, L. Zhao, J. Wu, R. Williams, and L. Perez, "A real-time rfid localization experiment using propagation models," in *Proc. IEEE Int. Conf. on RFID (RFID)*, 2012, pp. 141–148.

[69] Z. Yang, C. Wu, and Y. Liu, "Locating in fingerprint space: Wireless indoor localization with little human intervention," in *Proc. Proceedings IEEE MobiCOM*, 2012.

[70] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan, and R. Sen, "Zee: Zero-effort crowdsourcing for indoor localization," in *Proc. ACM MobiCOM*, 2012.

[71] T. Deyle, H. Nguyen, M. Reynolds, and C. Kemp, "Rf vision: Rfid receive signal strength indicator (rssi) images for sensor fusion and

mobile manipulation," in *Proc.IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, 2009, pp. 5553–5560.
[72] L. Ni, Y. Liu, Y. Lau, and P. Abhishek, "Landmarc: Indoor location sensing using active rfid," *Wireless Networks*, vol. 10, no. 6, pp. 701–710, 2004.
[73] Y. Zhao, Y. Liu, and L. M. Ni, "Vire: Active rfid-based localization using virtual reference elimination," in *Proc. Int. Conf. on Parallel Processing*, 2007.
[74] T. Nick, J. Gotze, W. John, and G. Stoenner, "Localization of uhf rfid labels with reference tags and unscented kalman filter," in *Proc. IEEE Int. Conf. on RFID-Technologies and Applications (RFID-TA)*, 2011, pp. 168–173.
[75] M. Khan and V. Antiwal, "Location estimation technique using extended 3-d landmarc algorithm for passive rfid tag," in *Proc. IEEE Int. Conf. on Advance Computing Conf.*, 2009, pp. 249–253.
[76] X. Chen, L. Xie, C. Wang, and S. Lu, "Adaptive accurate indoor-localization using passive rfid," in *Proc. IEEE Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2013.
[77] P. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao, "Phase based spatial identification of uhf rfid tags," in *Proc. IEEE Int. Conf. on RFID*, 2010, pp. 102–109.
[78] R. Miesen, F. Kirsch, and M. Vossiek, "Holographic localization of passive uhf rfid transponders," in *Proc. IEEE Int. Conf. on RFID (RFID)*, 2011, pp. 32–37.
[79] A. Wille, M. Broll, and S. Winter, "Phase difference based rfid navigation for medical applications," in *Proc. IEEE Int. Conf. on RFID (RFID)*, 2011, pp. 98–105.
[80] S. Azzouzi, M. Cremer, U. Dettmar, R. Kronberger, and T. Knie, "New measurement results for the localization of uhf rfid transponders using an angle of arrival (aoa) approach," in *Proc. IEEE Int. Conf. on RFID (RFID)*, 2011, pp. 91–97.
[81] Z. Babic, M. Ljubojevic, and V. Risojevic, "Indoor rfid localization improved by motion segmentation," in *Proc. 7th Int. Symp. Image and Signal Processing and Analysis (ISPA)*, 2011, pp. 271–276.
[82] W. Zhu, J. Cao, Y. Xu, L. Yang, and J. Kong, "Fault-tolerant rfid reader localization based on passive rfid tags," in *Proc. IEEE INFOCOM*, 2012, pp. 2183–2191.
[83] L. Yang, J. Cao, W. Zhu, and S. Tang, "A hybrid method for achieving high accuracy and efficiency in object tracking using passive rfid," in *Proc. IEEE Int. Conf. on Pervasive Computing and Commun. (PerCom)*, 2012, pp. 109–115.
[84] Y. Liu, L. Chen, J. Pei, Q. Chen, and Y. Zhao, "Mining frequent trajectory patterns for activity monitoring using radio frequency tag arrays," in *Proc. 5th Annu. IEEE Int. Conf. Pervasive Computing and Commun. (PERCOM)*, 2007.
[85] D. Zhang, J. Zhou, M. Guo, J. Cao, and T. Li, "Tasa: Tag-free activity sensing using rfid tag arrays," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 558–570, 2011.
[86] Y. Kawakita and J. Mitsugi, "Anti-collision performance of gen2 air protocol in random error communication link," in *Proc. Int. Symp. on Applications and the Internet Workshops*, 2006.
[87] M. Buettner and D. Wetherall, "An empirical study of uhf rfid performance," in *Proc. 14th Annu. Int. Conf. on Mobile Computing and Netw. (MobiCom)*, 2008.
[88] S. R. Aroor and D. D. Deavours, "Evaluation of the state of passive uhf rfid: An experimental approach," *IEEE Syst. J.*, vol. 1, no. 2, pp. 168–176, 2007.
[89] K. M. Ramakrishnan and D. D. Deavours, "Performance benchmarks for passive uhf rfid tags," in *Proc. 13th GI/ITG Conf. on Measuring, Modelling and Evaluation of Computer and Commun. Syst. (MMB)*, 2006.
[90] S. R. Jeffery, M. Garofalakis, and M. J. Franklin, "Adaptive cleaning for rfid data streams," in *Proc. 32nd Int. Conf. on Very Large Data Bases (VLDB)*, 2006.
[91] X. Xu, L. Gu, J. Wang, and G. Xing, "Negotiate power and performance in the reality of rfid systems," in *Proc. 8th Annu. IEEE Int. Conf. Pervasive Computing and Commun. (PerCom)*, 2010.
[92] X. Xu, L. Gu, J. Wang, G. Xing, and S. Cheung, "Read more with less: An adaptive approach to energy-efficient rfid systems," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1684–1697, 2011.
[93] W. Su, N. Alchazidis, and T. T. Ha, "Multiple rfid tags access algorithm," *IEEE Trans. Mobile Comput.*, vol. 9, no. 2, pp. 174–187, 2010.
[94] F. Achard and O. Savry, "A cross layer approach to preserve privacy in rfid iso/iec 15693 systems," in *Proc. IEEE Int. Conf. on RFID-Technologies and Applications (RFID-TA)*, 2012, pp. 85–90.
[95] J. Choi and C. Lee, "A cross-layer optimization for a lp-based multi-reader coordination in rfid systems," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2010, pp. 1–5.

Lei Xie received his B.S. and Ph.D. degrees from Nanjing University, China in 2004 and 2010, respectively, all in computer science. He is currently an associate professor in the Department of Computer Science and Technology at Nanjing University. His research interests include RFID Systems, Pervasive and Mobile Computing, and Internet of Things. He has published papers in IEEE Transaction on Parallel and Distributed Systems, ACM MobiHoc, IEEE INFOCOM, IEEE ICNP, IEEE ICC, IEEE GLOBECOM, MobiQuitous, etc. He is a member of ACM, IEEE and a senior member of CCF.

Yafeng Yin received her B.S. degree in computer science from Nanjing University of Science and Technology, China in 2011. She is currently a Ph.D. candidate in the Department of Computer Science and Technology at Nanjing University. Her research interests include RFID Systems, and Internet of Things.

Athanasios V. Vasilakos (M00CSM11) is currently a Professor with the University of Western Macedonia, Kozani, Greece. He served or is serving as an Editor or/and Guest Editor for many technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT; IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICSłPART B: CYBERNETICS; IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE; IEEE TRANSACTIONS ON COMPUTERS, ACM Transactions on Autonomous and Adaptive Systems; the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is also General Chair of the Council of Computing of the European Alliances for Innovation.

Sanglu Lu received her B.S., M.S. and Ph.D. degrees from Nanjing University, China in 1992, 1995 and 1997, respectively, all in computer science. She is currently a professor in the Department of Computer Science and Technology at Nanjing University. Her research interests include distributed computing and pervasive computing.