Distributed RFID Tag Storage Infrastructures

Technical Report
May 11, 2009

Victor K. Y. Wu*, Mirko Montanari, Nitin H. Vaidya, and Roy H. Campbell

University of Illinois at Urbana-Champaign, IL, USA
{vwu3, mmontan2, nhv, rhc,}@illinois.edu

Abstract. We leverage increasing passive RFID tag memory to propose distributed RFID tag storage infrastructures (D-RFID stores). A D-RFID store is a large set of tags with significantly sized re-writeable storage. Interrogators interact with D-RFID stores by reading from and writing to tags, providing a wide range of possible applications that are otherwise resource-inefficient. Examples include tagging trees in a forest to track hikers, interactive smart posters to provide location-based social interaction and collaboration, and tags transporting digital information in situations where reliable network connectivity is not available. We propose a system architecture for D-RFID stores by describing the tag distribution in space and time, different storage structures, and the middleware linking the different components together. We also describe assurance in our system. We motivate D-RFID stores through examples and describe potential avenues of research.

1 Introduction

Passive RFID (radio frequency identication) was originally envisioned as an identication technology aimed at replacing barcodes. Specically, EPCglobal has emerged as the organization tasked with developing RFID standards in this respect. Today, RFID is predominantly used by large companies such as Walmart and Walgreens to track tagged inventory [1], [2] and the containers carrying them (mobile asset management) [3]. The research community is also studying novel ideas and contexts (many even leading to fruition in the marketplace) for RFID beyond its original intended use. These include robotic tracking [4], tree logging [5], smart libraries [6], [7], and mobile payments using NFC (near field communications) [8].

Understandably, researchers and industry have paid little attention to fully exploiting RFID tag memory storage in a distributed manner. That is, the traditional paradigm of passive RFID dictates simplicity at the RFID tag level, and complexity at the RFID interrogator (reader) level. Passive tags are thought

* This work is supported in part by NSF grant CNS-0519817.

to be computationally limited, providing little storage beyond that for a single identifier. A interrogator scans tags for their identifiers, literally empowering the tags with its electromagnetic signal [9]. The interrogator then queries an online database to learn a plethora of information keyed to the tags' identifiers. More recently, the paradigm has shifted towards larger memory in tags, allowing for storage beyond merely identifiers. In [10], the author argues that extended storage allows tags to operate as "portable databases". As well, applications can still function if network access is not available, if most of the information relevant to the tagged item is in the tag itself. For example, auto manufacturers can use tagged parts in the assembly line [11]. The tags contain design specifications and are scanned by interrogators as a vehicle moves through the production line. RFID manufacturers are also responding to these ideas. GAO RFID and Atmel produce high frequency (13.56 MHz) tags with 10 thousand and 64 thousand bits of re-writeable storage, respectively [12], [13]. This is in stark contrast to EPCglobal UHF (ultra high frequency) Class 1 Gen 2 [14] compliant tags, which require only 96 bits for a unique identifier.

In this paper, we leverage increasing tag storage sizes to propose distributed RFID tag storage infrastructures (D-RFID stores). A D-RFID store is a large set of tags with significantly sized re-writeable storage, distributed in space and time. Interrogators interact with D-RFID stores by reading from and writing to tags. This provides a wide range of possible applications that are otherwise impossible or resource-inefficient. The required storage sizes of tags are dependent on the applications implemented on top of a D-RFID store.

Examples of such applications include tagging trees in a forest to track hikers. Hikers store their identifiers in tags as they move through the forest, forming a digital trail. When a hiker decides to leave the forest, he/she can backtrack, following the digital trail in reverse. Another example is using re-writeable tags in smart posters, as opposed to only readable tags. This allows for location-based social interaction and collaboration when people read from and write to the tags. A final example is using tags to carry digital information between senders and destinations in situations where reliable network connectivity is not available, such as ground zero at a disaster site, rural villages in developing countries, a military environment, or even a cruise ship. We exploit mobile entities (such as people or vehicles) carrying the tags to physically transfer the information, forming a communication network.

The rest of the paper is organized as follows. In Section 2, we propose a system architecture for D-RFID stores. We discuss the distribution of tags in space and time, how tags form different storage structures, and the middleware involved in linking the different components together. In Section 3, we describe reliability as well as privacy and security issues in our system. In these two sections, we provide brief examples to motivate D-RFID stores and also describe potential avenues of research. In Section 4, we detail the three aforementioned applications that leverage the benefits of our D-RFID store system architecture. Finally, we conclude in Section 5 and provide future work.

2 System Architecture

We describe the system architecture of a D-RFID store. We first discuss the distribution of tags in space and time, and also a third dimension, namely tag storage. Next, we discuss various storage structures that these tags support. These storage structures can further be organized as distributed databases. Finally, we discuss middleware, which links the different components together, and provides a design abstraction to applications.

2.1 Space, Time, and Storage

In a D-RFID store, a large set of tags are distributed in space. The authors in [15], [16] propose a "super-distributed" tag infrastructure. Citing the mu-Chip [17] as a small and inexpensive tag candidate, they envision deploying tags in space over large areas in a highly dense and redundant fashion. In applications built on top of such an infrastructure, the identity and behavior of a single tag becomes irrelevant, allowing for system robustness despite possible tag failures. Application performance depends on the system as a whole. Tags in D-RFID stores are generalized to have mobility patterns, similar to nodes in mobile ad hoc networks [18]. In other words, tags in a D-RFID store are distributed in space and time. Additionally, D-RFID stores further generalize super-distributed tag infrastructures by providing re-writeable storage. (The mu-Chip only has 128 bits for an identifier and no re-writeable storage, in contrast with the GAO RFID and Atmel tags mentioned above.) We characterize the state $x_i(t)$ of tag i at time t as:

$$x_i(t) = (p_i(t), s_i(t), r_i(t)), \tag{1}$$

where $p_i(t)$ is the location of tag i at time t, at which it is carrying $s_i(t)$ bits of storage out of a possible capacity of $r_i(t)$ bits, where $i \in \{1, \ldots, n\}$, if there are n tags. ($s_i(t)$ can be further reduced to storage specific for different applications.) The state $X(t)$ of the D-RFID store is the collection of all tag states. That is, $X(t) = (x_1(t), \ldots, x_n(t))$.

Future research includes characterizing feasible D-RFID store states for different applications and their deployment. For example, similar to [15], [16], tags in a location system are embedded in the floors of a building, each storing its location. Mobile entities (people, robots, etc.) carrying RFID interrogators locate themselves by scanning tags. Since tags are stationary, $p_i(t) = p_i$. In this situation, tags cannot be positioned too sparsely, since this results in inaccurate location information. Tags positioned too densely potentially confuse users, since too many tags may respond to a single interrogator scan. This constrains possible values for p_i. $s_i(t) \in \{0, l\}$, where l is the size of a location coordinate, and $r_i(t) = l, \forall t$. That is, a tag either stores its location or is empty. (Note that tags do not require unique identifiers for this application.)

2.2 Data Structures

Each RFID tag can only provide a limited amount of storage. Efficiently storing information on the RFID tags represents a challenge. On one hand, a standard format such as XML [19] guarantees interoperability between different applications and different implementations of the D-RFID store architecture, but it requires more storage. (Techniques such as XML-specific compression [20] could be applied to provide substantial reduction of the space footprint.) Conversely, however, other formats, such as a flat representation of data in a fixed predefined format, can provide higher efficiency storage for specific applications.

We can also use multiple tags to store complex data in a D-RFID store. For example, a large data structure can be represented as a linked list. Each tag represents a node in the linked list. Therefore, in addition to storing a piece of information, a tag also has to have a pointer to the next node (tag) in the linked list. This can be the tag identifier of the next tag. Alternatively, the pointer can be the physical location coordinates of the next tag. In this way, an interrogator can read from and write to data using the pointers. This is generalized to more complex data structures such as trees or graphs, where each tag may have multiple pointers to other tags.

A frequent operation performed on data structures is searching. If the data is keyed in some fashion, a hash table is a search-efficient data structure that can easily be adapted for D-RFID stores. For example, suppose we are storing personal information (sex, birth date, etc.) keyed to people's names. We hash the name of a person to an index that ultimately determines (fully or in part), the tag or tags where that person's information is stored. That is, the hash index may be a tag identifier or the location coordinates of a tag. In a larger D-RFID store, the hash index may only specify the general location in space. A further mechanism may be used (a linked list for instance) to store or retrieve information on a tag or tags at that general location.

In general, information is stored over multiple tags in space. That is, we are spatially encoding the data for a variety of reasons, including compression to save storage and redundancy to fight against tag failures, and channel unreliability (to be discussed in more detail in Section 3). Future research includes investigating these two types of encoding (namely, source and channel coding), and if there exists some relationship between them, similar to perhaps the source-channel separation theorem [21] in information theory.

The architecture of the D-RFID store allows applications to be abstracted away from the low level mechanism used to encode and save data on the tags. The next section describes how our proposed architecture allows changes in the low level representation of the data without affecting applications.

2.3 Distributed Databases

If the D-RFID store is viewed as a repository of information, the connection of this concept with a database system becomes evident. The entire collection of information stored in an area can be seen as a large geographically distributed

database that can be interrogated to extract and update information. Previous research in wireless sensor networks analyzes the problem of storing information in a geographically distributed area. Solutions such as TinyDB [22] and Cougar [23] provide systems for interrogating data stored in a network of distributed sensors. This data, called the "sensor database", are accessed through the use of declarative languages similar to SQL. As the main purpose of sensor nodes is to collect information from the environment, those languages incorporate statements for specifying sampling periods and data aggregation.

The D-RFID store architecture creates new challenges in the application of those methodologies. RFID tags, as passive platforms, do not have the ability to exchange data directly. All the active actions need to be performed by an RFID interrogator that moves in the area, in an attempt to access the information contained in the RFID tags in range. However, this information is not readily available for access, but instead they need to be "sampled" by a RFID interrogator. That is, each RFID tag can be seen as a tuple with an attribute $p_i(t)$ that represents its location at time t and a set of data $d_i(t)$ stored at the tag. Using a declarative language like SQL, users have the ability, for example, to query the position of RFID tags containing a certain information at time t (and potentially update it) or to find and update the information stored in the tags that are at a particular location at time t. By taking advantage of the structure of the information $d_i(t)$, the query language can be extended to perform complex operations such as aggregation and filtering. Using the D-RFID store data model for accessing data, writing in the tags can be represented as a SQL UPDATE instruction. RFID tags are first identified using a SELECT over the D-RFID store with conditions specified over geography, time and data. The selected tags can be updated with the information specified in the UPDATE statement. However, further research needs to address the consistency requirements that certain applications might have on the data stored on multiple RFID tags.

When we take into account the location of RFID tags and interrogators as part of the data model, the information contained in the D-RFID store can be seen as continuously changing. Instead of searching for information, people can be interested in "events", that is, a particular piece of data becomes available at a certain location. Recent work on large scale publish/subscribe systems can be extended to this environment [24]. The publish/subscribe architecture provides a model where each application using the D-RFID store can be a subscriber and specify their interests (also called subscriptions or continuous query) using a declarative language. The subscription can specify which type of information the application is interested in. For example, an application can be interested in all the information available on tags placed in a particular geographic area and that has been saved in the last day. When the RFID interrogator finds a tag with location and content matching the subscription, an event is generated and all subscribed applications are notified. Efficiently interrogating and updating the information contained in the geographically distributed D-RFID store is a challenging issue and requires interrogation advancements in publish/subscribe

systems, distributed databases and opportunistic sensing to be performed efficiently. For example, further research can aim at optimizing the energy consumed by RFID interrogators in performing its operations. Knowledge about the subscription and about contextual information, such as the location of D-RFID interrogators, enable the system to interrogate for the presence of tags only when there is at least one application interested in such data. Interpreting the D-RFID store as a large database interrogated through declarative languages allows abstracting the encoding of the information from the specific applications. Even though passive tags are increasingly providing more storage, they lag behind active devices in this respect. Therefore, optimizations can be integrated in the encoding of the information to reduce its footprint in a way transparent to applications.

2.4 Middleware

Previous work in RFID middleware focuses on the requirements of traditional RFID applications (for example, interrogating tags in a warehouse for inventorying) and the constraints of the RFID physical channel [25]. In particular, the massive amounts of data collected by interrogators has to be filtered [26], [27] before it is recognizable to the higher layers in such applications. In D-RFID stores, we find similar challenges. Additionally, our middleware needs to be suitable for an even wider range of applications, providing a sufficient abstraction to simplify the use of a D-RFID store, but at the same time, it must also efficiently use the limited storage available in the tags. Further research includes developing such a rich but lean middleware. In the following, we only briefly outline a D-RFID middleware and highlight some relavent issues.

Using a simple model, the D-RFID store middleware can be structured in a set of layers: an application interface, a data model, a coding layer and a physical layer. The application interface provides a common API to applications reading from and writing information to the D-RFID store. Applications can specify the information to write, the location and the time at which the information needs to be written using a predefined declarative structure, e.g. XML or tuple based. The declarative specification is then passed to the data model layer that transforms it into a standard binary representation suitable for the small space available on tags. This stream of bits is then encoded by the coding layer to obtain the required level of error resistance, as explained in Section 3.2, and then written on the tags by the physical layer.

The access to data follows a similar path. We envision two models for accessing the data: a pull method and a push method. Using the pull method, the application can request access to information using an SQL-like declarative language. The request is passed to the data model and the coding layer that transforms it into a physical read request from a set of tags. The information stored in the tags is then decoded by the coding layer and interpreted using the standard format defined in the data model. This information is then passed back to the application. In the push method, the application can provide subscriptions to particular data. These subscriptions are stored in the data model layer

that coordinates the reading of tags with the coding and the physical layers. When new information corresponding to the subscription enters in range, the data model notifies the application through an event-based interface.

An advanced middleware can also coordinate the sharing of information between RFID interrogators. Information about geographically remote tags can be obtained by aggregating information coming from multiple interrogators. These RFID interrogators can be seen as nodes in a Mobiscope [28] that collect information in an opportunistic or participatory way [29], [30]. Interrogators placed on mobile platforms (e.g., mobile phone) can collect information about RFID tags while users move in the environment. Information collected by the single RFID interrogator can be shared and used to respond to queries submitted by other individuals. Research in the area of aggregating and sharing sensor data [31] can be extended to the case where other information (and not only sensor data) is physically embedded in the environment. Further research will explore how to access information in an efficient way. Not all information needs to be collected at the same time, and not all RFID interrogators need to be activated in the same area to collect the required information.

3 System Assurance

We describe assurance in a D-RFID store. Specifically, we discuss tags failing due to the physical environment, unreliability in the storage and retrieval process, and attacks on privacy and security of a D-RFID store. We discuss methods to defend against such risks.

3.1 Tag Reliability

In many applications, tags are deployed in harsh physical environments. Changes in the ambient temperature, pressure, or humidity may damage tags. For instance, in a disaster situation with burning environments, tags are deployed for search and rescue purposes [32], and are destroyed after heating up over time. Future research includes characterizing tag failures, in order to design robust D-RFID stores.

3.2 Storage and Retrieval Reliability

D-RFID stores are used for distributed storage. In particular, suppose an interrogator stores information in a set of tags at time 0. At time t, it attempts to retrieve the information. However, the retrieval may be unreliable due to tag failures. We thus view this storage and retrieval as an unreliable channel, in the information theoretic sense. Future research includes characterizing this channel (including its capacity) due to different sources of unreliability as well as developing channel codes that combat this unreliability, in order to approach capacity.

For example, consider tags occasionally failing with increasing probability over time (unlike the failure model in Section 3.1, where failures are permanent). Suppose an interrogator completely writes to a set of tags $\{i\}_{i=1}^{n}$ at time 0 with perfect reliability. Independent information is stored in each tag. We have $s_i(0) = r_i(0) = u$, according to (1), where u is the storage size of every tag. At time $t > 0$, the interrogator scans the set of tags. Due to failures, tag i responds with probability $e^{-t\alpha_i}$, where $\alpha_i > 0$ can be viewed as the time exponential rate at which tag i becomes more prone to failures. (α_i models the effects of the physical environment on tag i, similar to the burning environment example in Section 3.1.) If a tag does not respond, the interrogator does not retrieve the tag's storage. Therefore, the channel capacity is $C(t) = \sum_{i=1}^{n} e^{-t\alpha_i} u$ bits. Note that $\lim_{t\to 0} C(t) = nu$ and $\lim_{t\to\infty} C(t) = 0$. That is, the channel capacity (information retrievability) degrades over time.

Other sources of unreliability include tag and interrogator mobility. If the set of tags move far away from the interrogator or disperse over a large area by time t, in relation to the interrogator's own trajectory in that period, then the interrogator cannot retrieve much of the storage. However, if the set of tags and the interrogator congregate in space at a later time after t, the interrogator can once again retrieve the storage. In other words, $C(t)$ is not necessarily a monotonically decreasing function in time. Additionally, depending on the system protocols, existing tag storage may be overwritten by other interrogators, further decreasing the channel capacity. Finally, unreliability can stem from interference due to multiple tags and interrogators. When there is one interrogator scanning multiple tags, the tags must coordinate themselves in a distributed manner to minimize interference when responding. Deterministic solutions to this problem include tree-based schemes [33] while probabilistic solutions are similar to Aloha [34]. When there are multiple interrogators, the interrogators themselves have to minimize interference from each other. Solutions to this "reader (interrogator) collision problem" [35] include graph coloring-based approaches [36].

Future research includes developing channel codes (error control codes) to combat the unreliability in the information retrievable process. That is, we wish to introduce controlled redundancy in the storage to achieve a minimum reliability requirement (for example, maximum allowed bit error/erasure rate). For instance, suppose we know that tags fail permanently after an exponential time, according to the description in Section 3.1. Or suppose tags become increasingly prone to occasional failures over time, as detailed above. Then, an interrogator can choose the tags with lower failure probabilities when storing information. The interrogator can also store the same information in multiple tags. For example, if we know that tags close to each other are affected by similar physical effects (such as temperature, pressure, or humidity), then the interrogator should choose to store information in tags that are far apart from each other. The tradeoff of course is that the interrogator has to move to multiple locations when storing and retrieving information.

Traditional storage systems naturally use error control codes. For example, error bursts are common in computer hard disks and optical media, due to

dust particles and scratches. Reed-Solomon codes are often candidates in such systems [37], [38]. In D-RFID stores, burst errors can also occur, due to sudden changes in the environment, affecting a fraction of the tags in a small physical locality. Future research includes investigating the similarities of D-RFID stores with other storage systems to see if any existing results (such as error burstiness and Reed-Solomon codes) can be re-applied.

3.3 Privacy and Security

Researchers and industry experts are concerned with the privacy and security of RFID tags, and more specifically the objects to which they are affixed. For example, an attacker uses an interrogator to scan the EPC code [39] of a tag affixed to a pallet of goods in a shipping depot in City A, and he/she determines that the pallet contains Company X running shoes that are destined for a Company Y retail outlet in City B. Later on, a collaborating attacker scans the same pallet as it is moved into the Company B warehouse, confirming the running shoes' arrival. In other words, the privacy of: (1) the identity of the tagged object(s) (running shoes), (2) the manufacturer (Company X), (3) the retailer (Company Y), and (4) the path (City A to City B) is compromised. Specifically, we are concerned with protecting the contents of an RFID tag (it's identifier, which can be keyed to learn information about its information), and protecting the path of travelled by the tag. These are called inventorying and tracking/location privacy, respectively. [40]. Since passive tags are computationally weak, cryptogrphic methods used in computer security are not readily applied to protect RFID privacy. Instead, the literature investigates a variety of issues and solutions appropriate for passive tags. In [41], tags cycle through a list of pseudonyms when responding to interrogators. Friendly interrogators have the entire list, enabling them to identify tags. Malicious interrogators do not, and thus are confused by the continually changing responses. In [42], tags respond slowly to interrogations, decreasing the chances of an attacker acquiring tag identifiers. Friendly interrogators use caching to quickly scan tags. In [43], the authors investigate the problem of transferring tag ownership (for example at a retail point of sale) and provide protocols protecting the privacy of the old and new owners.

In D-RFID stores, these privacy and security requirements obviously still apply. However, we are additionally concerned with the confidentiality, integrity, and availability [44] of tag storage. For example, to protect the confidentiality of storage, an interrogator encrypts the information using a symmetric key before writing it to the tags. At a later time, it retrieves the encrypted data and decrypts it to recover the information. Integrity in our case can refer to the source of the data, that is, the interrogators. For example, suppose that a section of a D-RFID store is rented to a specific patron as storage. The tags making up that section therefore must authenticate any interrogator reading from and writing to them, using perhaps, a password initialized at rental time. The interrogator must also authenticate the set of tags, since attackers (which are active devices in general) may masquerade as tags after cloning them [45]. Finally, the availability of storage may be affected because of tag failures, due to the physical environment,

as mentioned in Sects. 3.1 and 3.2, or attackers actively a launching a denial-of-service attack. For example, malicious interrogators may create interference on the RFID wireless channel in an area by transmitting high power signals. To protect availability, the interrogator can store information in tags that are far apart from each other, as explained in Section 3.2. This assumes that a large number of malicious interrogators are not available to collaborate over a large space without quickly being detected by the proper authorities, similar to the weakened attacker model in [41].

Even though many traditional notions in computer security may be not be applicable to passive RFID (as mentioned above), they may nonetheless be well-suited in a D-RFID store with significant amounts of re-writeable storage. For example, in a (n, t) secret sharing scheme [46], a secret is divided into n shares and distributed. If and only if at least $t \leq n$ shares are recovered, the secret can be reconstructed. In a D-RFID store, the n shares of a secret (a company's formula for a popular beverage for instance) can be first encrypted using n symmetric keys, and stored in n distinct tags. The chief executive officer is given t symmetric keys. This allows him/her to recover the secret by him/herself. Other executives are given fewer (and distinct) symmetric keys each, requiring them to collaborate, in the event that the chief executive officer is not available. This is similar to an example in [46].

Future research includes further characterizing the privacy and security issues in D-RFID stores.

4 Applications

We propose several applications that leverage the salient features of a D-RFID store. These applications further motivate research in the aforementioned areas. In particular, they can be rapidly developed using the middleware in Section 2.4, hiding the D-RFID details in Section 2 from the system designer.

4.1 Tagging Trees to Track Hikers

In [47], we propose embedding RFID tags in trees in a forest to track hikers, forming the D-RFID store. Hikers use RFID interrogators embedded in their mobile phones to read from and write to tags. As a hiker moves through the forest, he/she stores his/her unique identifier in tags, forming a digital trail. (We assume tags can store many identifiers, and multiple tags can be embedded in a tree. This is in contrast to [15], [16], where the mu-Chip is cited for its advantageous small size, but has little storage in it.) When he/she decides to leave the forest, he/she backtracks, following the digital trail in reverse. (In general, hikers do not need to physically see or know which specific trees the tags are embedded in. Using UHF RFID, an interrogator scans a large area, reading from and writing to tags in the vicinity as the hiker moves through the forest.) The trails can also be used to follow hikers, in the case of search and rescue of a missing hiker, for example. This application highlights many

benefits of a D-RFID store, since in a forest, it is very difficult to install a tracking system using traditional digital means. For example, the authors in [48] propose an unrealistic system called CenWits. In CenWits, each hiker wears a GPS (global positioning system) receiver and a short range transceiver. When hikers come in contact with each other, they become location witnesses for each other by exchanging location information (retrieved from the GPS receivers) using their transceivers. Dedicated access points are installed throughout the forest, with connections to a central server. When a hiker passes by an access point, he/she uploads his/her accumulated location history information (about him/her and hikers he/she previously encountered). If a hiker becomes lost, first responders can be deployed using location information from the central server. CenWits requires GPS, which may not function in a highly wooded area. Our D-RFID store solution does not require any explicit location determination system. Futhermore, CenWits requires installing and maintaining expensive access points at well-known locations, making the system not robust and unscalable as the hiker population increases. In contrast, very minimal cost is required to install our D-RFID solution. For example, the forest authorities are responsible for embedding the tags. Alternatively, hikers themselves acquire the inexpensive tags and embed them in trees as they move through the forest. Maintaining tags costs virtually nothing. If tags fail (which occur only occasionally in space and time) or the number of hikers increases, more tags can be added, allowing for a robust and scalable system. Our D-RFID store backtracking system also encourages collaboration between hikers. Hikers can store location-specific information in tags, such as maps or ratings of specific hiking paths. This allows for dynamic communication between hikers in space and time. We note that in a forest, network connectivity is expensive to install and maintain (as proposed in [48]). Our system stores information "inline" and requires no maintenance at all.

4.2 RFID Whiteboards for Location-based Interaction and Collaboration

Hiker collaboration using tags embedded in trees is further generalized to "RFID whiteboards". That is, re-writeable tags are installed in public places. People equipped with RFID interrogators read from and write to the tags, allowing for a variety of location-based, interactive and collaborative applications. For example, users equipped with NFC devices typically only read information from an NFC smart poster [49]. For instance, a movie poster may direct an NFC-enabled smart phone to a website containing promotional materials and local show times. Alternatively, we propose using re-writeable tags in the smart poster. The smart poster now serves as a local forum, where movie-goers can post and read movie reviews. The system provides location-based, social interaction for movie goers and is simple to install. Movie-goers are more likely to use the system, since it obviates the need for registration typically found in an online forum. Network connectivity is not required, as the social experience is focused on the immediate physical locality. Movie-goers may even interact with multiple movie posters in the cinema, thus creating and moving information over many

tags. For example, movie-goers may collaboratively vote over time on the best movie currently playing in a cinema by writing their votes in tags. The D-RFID store in such a situation is the collection of all NFC tags in the entire cinema.

Digital social interaction and collaboration has flourished on the Internet in the form of social and business networks. As mobile technology (infrastructure, devices, software, and hardware) and mobile businesses continue to mature, the focus is shifting to location-based applications. One of the paradigms of this mindset is associating physical locations or objects with online identities and/or information repositories, thus enhancing the physical world with a set of feature-rich applications. While we agree with such a philosophy, there are nonetheless many situations where network connectivity is impossible or cost-prohibitive, given the application requirements. In these cases, we argue that D-RFID stores with sufficient storage allow applications to be built that provide simple, intuitive and rich user experiences that are fundamentally location-based and collaborative.

4.3 Communication without Connectivity

In a D-RFID store, a large set of tags are distributed in space and time. Interrogators interact with the D-RFID store by reading from and writing to tags. Depending on the particular application, we can view the D-RFID store and/or interrogators as nodes in a mobile ad hoc network. For example, consider situations where reliable network connectivity is unavailable. This may be ground zero at a disaster site, rural villages in developing countries, a military environment, or even a cruise ship. Delay tolerant networks are often built in such situations [50], [51], [52] to provide communication even under such dire conditions. For example, DakNet [53] is providing Internet connectivity to remote areas in India and Cambodia. In DakNet, mobile access points (in the form of buses or motorocyles) carry digital information between a city with Internet access and villages. This physical transport of data provides higher throughputs (20 Megabytes in each direction) than a telephone modem. Alternatively, we can use tags to carry the information, similar to message ferries [54], [55]. Similar to the tree tagging application above, inexpensive tags are easily deployed, have virtually zero maintain cost, and the number of tags is easily scaled to meet the traffic demands.

The authors in [56] implement a delay tolerant network protocol for mobile phones. The sender first records an audio message on his/her mobile phone. The message is then wirelessly forwarded asynchronously through several intermediate phones (via Bluetooth or other technologies) before arriving at the destination's phone. Such a protocol could be useful in a cruise ship where cellular telephony is unavailable. Instead, suppose cruise patrons are provided with inexpensive RFID tags with re-writeable storage. They are embedded in items commonly carried by a patron, such as the patron identifier card, food and drink containers or clothing bought on board. A cruise patron uses his/her mobile phone to broadcast a message to tags (write to tags via the RFID channel) carried by neighboring patrons. If a neighboring patron eventually moves to the

vicinity of the intended receiver, the message can be delivered by the receiver's mobile phone reading the tag.

We envision RFID tags becoming much more prevalent in the future. People will carry them unknowingly. They will be embedded in clothing, wallets, purses, and electronic devices. These tags will often contain unused re-writeable storage as passive RFID tag technology develops, as mentioned in Section 1. If the RFID community agrees on standards for accessing such unused storage, the storage can be used dynamically by RFID interrogators as a communications medium or for other purposes, similar to how cognitive radios search for available spectrum. We also envision RFID interrogators increasingly being integrated into mobile phones. The mobile phone has matured into a ubiquitous communications and computing device, guaranteeing a user to always carry one. Currently, Nokia, Samsung, LG, and Motorola all offer NFC-enabled handsets [57]. Nokia has even integrated a UHF interrogator into one of its handsets [58]. [59] and [60] offer interrogator software used in mobile phones. In other words, we see RFID tags and mobile phones forming dense mobile ad hoc networks in public places, in the near future.

Future research includes characterizing a D-RFID store as a manifestation of a network. This allows existing networking theory to be leveraged for investigation and design of D-RFID stores for different applications. That is, protocols and results (analytical and experimental) from networking research can be used to study throughput, delay, routing, etc. for information flowing through a D-RFID store. For example, the authors in [61] show that if n nodes in a wireless network are randomly located, the throughput achievable by each node to a random destination is $\Theta\left(\frac{1}{\sqrt{n \log n}}\right)$. [62] extends [61]'s work to show node mobility further improves the throughput. If tags and/or interrogators are treated as nodes, we may find similar results in the scaling behavior.

5 Conclusion and Future Work

In this paper, we leverage increasing tag storage sizes to propose D-RFID stores. We argue that such systems provides a wide range of possible applications that are otherwise impossible or resource-inefficient. We provide a system architecture as well as a discussion on assurance issues. Through example applications we motivate and discuss potential avenues of research according to this new paradigm.

Future work involves engaging the research community to work on the problems presented herein. This includes researching theoretical foundations in order to determine the fundamental efficiency limits in D-RFID stores, as well as developing engineering optimizations to approach those limits. At the same time, we (as a research community) need to develop middleware to implement these ideas. As an open source project, both academic institutions and industry organizations need to be actively involved in this process. In particular, AspireRFID [63] is already leading an open source middleware effort. Nonetheless, we need additional code to support the multiplicity of tags and storage, as envisioned in

the D-RFID store model. Finally, real-life applications of D-RFID stores have to be tested and eventually deployed. Thereafter, we need large scale user studies to validate our applications and infrastructures, in order to refine our systems as necessary.

References

1. "RFID News: Looking Back at the Wal-mart RFID Time Line," *Supply Chain Digest*, Feb. 2009. Available: http://www.scdigest.com/assets/newsviews/09-02-23-1.pdf
2. "Walgreens: RFID Promotions Tracking a "Game-Changer"," *RFID Update*, Mar. 2009. Available: http://www.rdupdate.com/news/03032009.html
3. T. Inaba, "Value of Sparse RFID Traceability Information in Asset Tracking during Migration Period," in*Proc. IEEE International Conference on RFID*, Las Vegas, NV, Apr. 2008, pp. 183-190.
4. D. Hahnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, "Mapping and Localization with RFID Tehcnology," in *Proc. IEEE International Conference on Robotics and Automation*, New Orleans, LA, Apr. 2004, vol. 1, pp. 1015-1020.
5. "In the Forest," *Discover RFID*. Available: http://www.discoverrfid.org/what-is-possible/work-better/in-the-forest.html
6. K. G. Schneider, "RFID and Libraries: Both Sides of the Chip," California Library Association Intellectual Freedom Committee, Nov. 2003.
7. "LibBest Library Information System", BookTec Information Company. Available: http://www.rd-library.com/
8. "Proximity Mobile Payments: Leveraging NFC and Contactless Financial Payments Infrastructure", Smart Card Alliance, Sep. 2007.
9. D. M. Dobkin, *The RF in RFID*. Oxford, UK: Elsevier, 2008.
10. S. Liu, "Extended Memory RFID Tags Provide Immediate Access to Data Anywhere, Anytime," *Intelleflex*, 2007. Available: http://www.industrial-embedded.com/pdfs/Intelleflex.Win07.pdf
11. Z. Li, R. Gadh, and B. S. Prabhu, "Applications of RFID Technology and Smart Parts in Manufacturing," in *ASME Proc. Design Engineering Technical Conferences (DETC)*, Salt Lake City, UT, Sep.-Oct. 2004.
12. "13.56 MHz high frequency (HF) rectangle paper RFID tag," *GAO RFID*. Available: http://www.gaorfid.com/index.php?main_page=index&cPath=68
13. "13.56 MHz CryptoRF EEPROM Memory 64 Kbits", *Atmel*. Available: http://www.atmel.com/dyn/resources/prod_documents/5006s.pdf
14. "EPCglobal UHF Class 1 Gen 2," *EPCglobal*. Available: http://www.epcglobalinc.org/standards/uhfc1g2
15. J. Bohn and F. Mattern, "Super-distributed RFID Tag Infrastructures," *Lecture Notes in Computer Science*, vol. 3295, pp. 1-12, 2004.
16. J. Bohn, "Prototypical Implementation of Location-Aware Services based on a Middleware Architecture for Super-Distributed RFID Tag Infrastructures," *Lecture Notes in Computer Science*, vol. 3894, pp. 69-83, 2006.
17. "The World's Smallest RFID IC mu-Chip," *Hitachi*. Available: http://www.hitachi.co.jp/Prod/mu-chip
18. T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models in Ad Hoc Network Research," *Wireless Communications and Mobile Computing: Special Issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483-502, Aug. 2002.

19. "W3C Extensible Markup Language (XML)".
Available: http://www.w3.org/XML/
20. H. Liefke and D. Suciu, "XMill: an efficient compressor for XML data," in *ACM SIGMOD Record*, vol 29, no. 2, pp 153–164, 2000
21. C. E. Shannon, "A Mathematical Theory of Communication," *Bell Systems Technical Journal*, vol. 27, pp. 379-423, Jul. 1948.
22. S. R. Madden, M. J. Franklin, and J. M. Hellerstein, "TinyDB: An Acquisitional Query Processing System for Sensor Networks," in *ACM Transactions on Database Systems*, vol. 30, 2005, pp. 122-173.
23. P. Bonnet, J. Gehrke, and P. Seshadri, "Towards Sensor Database Systems," *Lecture Notes in Computer Science*, Springer, 2001, pp. 3-14.
24. A. Demers, J. Gehrke, B. Panda, M. Riedewald, V. Sharma, and W. White, "Cayuga: A General Purpose Event Monitoring System," in *Proc. Biennial Conference on Innovative Data Systems Research (CIDR)*, Asilomar, CA, 2007, pp. 412-422.
25. C. Floerkemeier and M. Lampe, "RFID Middleware Design - Addressing the Application Requirements and RFID Constraints," in *Proc. ACM Joint Conference on Smart Objects and Ambient Intelligence*, Grenoble, France, Oct. 2005, pp. 219-224.
26. F. Wang and P. Liu, "Temporal Management of RFID Data," in *Proc. International Conference on Very Large Data Bases*, Trondheim, Norway, Aug.-Sep. 2005, pp. 1128-1139.
27. S. Jeffery, M. Garofalakis, and M. J. Franklin, "Adaptive Cleaning for RFID Data Streams," in *Proc. International Conference on Very Large Data Bases*, Seoul, Korea, Sep. 2006, pp. 163-174.
28. T. Abdelzaher, Y. Anokwa, J. Burke, D. Estrin, L. Guibas, A. Kansal, S. Madden, and J. Reich, "Mobiscopes for Human Spaces," *IEEE Pervasive Computing*, vol. 6, p. 20, 2007.
29. A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-Centric Urban Sensing," *Proc. ACM International Workshop on Wireless Internet*, New York, NY, 2006.
30. J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory Sensing," *World Sensor Web Workshop*, 2006, pp. 1-5.
31. S. Nathm J. Liu, F. Zhao, "SensorMap for Wide-Area Sensor Webs," *IEEE Computer*, vol. 40, number 7, pp. 90-93, Jul. 2007.
32. A. Kleiner, J. Prediger, and B. Nebel, "RFID Technology-based Exploration and SLAM for Search and Rescue," in *Proc. IEEE International Conference on Intelligent Robots and Systems (IROS)*, Beijing, China, Oct. 2006, pp. 4054-4059.
33. C. Law, K. Lee, and K.-Y. Siu, "Efficient Memoryless Protocol for Tag identification," in *Proc. ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIALM)*, Boston, MA, Aug. 2000, pp. 75 - 84.
34. H. Vogt, "Multiple Object Identification with Passive RFID Tags," in *Proc. IEEE International Conference on Systems, Man and Cybernetics (SMC)*, Hammamet, Tunisia, Oct. 2002.
35. D. W. Engels, "The Reader Collision Problem," *White Paper*, Nov. 1, 2002. Available: http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-007.pdf
36. J. Waldrop, D. W. Engels, S. E. Sarma, "Colorwave: a MAC for RFID reader networks," *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, Mar. 2003, vol. 3, pp. 1701-1704.
37. E. Fujiwara, D. K. Pradhan, "Error-Control Coding in Computers," *IEEE Computer*, vol. 23, no. 7, pp. 63-72, Jul. 1990.

38. D. J. Costello Jr., J. Hagenauer, H. Imai, and S. B. Wicker, "Applications of Error-Control Coding," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2531-2560, Oct. 1998.
39. "EPC Essentials," *EPCglobal*. Available: http://www.epcglobalinc.org/consumer_info/essentials/
40. A. Juels, "RFID Privacy and Security: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394 Feb. 2006.
41. A. Juels, "Minimalist Cryptography for Low-cost RFID Tags," in *Proc. of Security of Communication Networks (SCN)*, Amalfi, Italy, Sep. 2004, pp. 149-164.
42. M. Langheinrich and R. Marti, "Practical Minimalist Cryptograph for RFID Privacy," *IEEE Systems Journal*, vol. 1, no. 2, pp. 115-128, Dec. 2007.
43. B. Song, "RFID Tag Ownership Transfer," in *Proc. of Workshop on RFID Security (RFIDSec)*, Budapest, Hungary, Jul. 2008.
44. M. Bishop, *Introduction to Computer Security*. Addison-Wesley Professional, 2004.
45. A. Juels, "Strengthening EPC Tags Against Cloning," in *Proc. ACM Workshop on Wireless Security (WiSe)*, Cologne, Germany, Sep. 2005, pp. 67-76.
46. A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.
47. V. K. Y. Wu, N. H. Vaidya, and R. H. Campbell, "RFID Trees: A Distributed RFID Tag Storage Infrastructure to Backtrack Hikers in a Forest," *Technical Report*, Apr. 2009. Submitted to *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, Oct. 2009. Available: http://www.crhc.illinois.edu/wireless/papers/tech_report_victorwu_rfid_trees.pdf
48. J.-H. Huang, S. Amjad, and S. Mishra, "CenWits: A Sensor-based Loosely Coupled Search and Rescue System using Witness," in *Proc. ACM Conference on Embedded Networked Sensor Systems (SenSys)*, San Diego, CA, Nov. 2005, pp. 180-191.
49. "NFC Smart Poster RTD Technical Specification". Available: http://www.nfc-forum.org/specs/spec_list/
50. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," in *Proc. ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Karlsruhe, Germany, Aug. 2003, pp. 27-34.
51. S. Jain, K. Fall, R. Patra, "Routing in a Delay Tolerant Network," in *Proc. ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Portland, OR, Aug.-Sep. 2004, pp. 145-158.
52. S. Jain, M. Demmer, R. Patra, and K. Fall, "Using Redundancy to Cope with Failures in a Delay Tolerant Network," *Computer Communication Review*, vol. 35, no. 4, pp. 109-120, Oct. 2005.
53. A. Pentland, R. Fletcher, and A. Hasson, "DakNet: Rethinking Connectivity in Developing Nations," *IEEE Computer*, vol. 37, no. 1, pp. 78-83, Jan. 2004.
54. W. Zhao and H. Ammar, "Message Ferrying: Proactive Routing in Highly-partitioned Wireless Ad Hoc Networks," in *Proc. IEEE International Workshop on Future Trends in Distributed Computing Systems (FTDCS)*, San Juan, Puerto Rico, May 2003, pp. 308-314.
55. W. Zhao, H. Ammar, and E. Zegura, "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Tokyo, Japan, May 2004, pp. 187-198.
56. M. T. Islam, "DT-Talkie: Interactive Voice Messaging for Heterogeneous Groups in Delay Tolerant Networks," in *Proc. IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, Jan. 2009.

57. "NFC research: Devices," *Near Field Communication Research Lab.* Available: http://www.nfc-research.at/index.php?id=45
58. J. T. Savolainen, H. Hirvola, and S. Iraji, EPC UHF RFID Reader: Mobile Phone Integration and Services, in *Proc. IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, Jan. 2009.
59. A. Löfer, U. Wissendheit, H. Gerhäuser, and D. Kuznetsova, GIDS - A System for Combining RFID-based Site Information and Web-based Data for Virtually Displaying the Location on Handheld Devices, in *Proc. IEEE International Conference on RFID*, Las Vegas, NV, Apr. 2008, pp. 312319.
60. L. Pohjanheimo, H. Keränen, and H. Ailisto, Implementing TouchMe Paradigm with a Mobile Phone, in *Proc. ACM International Conference on Smart Objects and Ambient Intelligence*, vol. 21, Grenoble, France, Oct. 2005, pp. 8792.
61. P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388-404, Mar. 2000.
62. M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad-hoc Wireless networks," in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, Anchorage, AK, Apr. 2001, vol. 3, pp. 1360-1369.
63. "AspireRFID Middleware Wiki."
Available: http://wiki.aspire.ow2.org/xwiki/bin/view/Main/