A Scalable, Privacy-Preserving and Secure RFID Protocol

Charles Mutigwe, Farhad Aghdasi, and Johnson Kinyua

***Abstract*—In this paper we propose a communication protocol for Radio Frequency Identification (RFID) systems that is based on the tags responding only to authenticated readers, otherwise tags always maintain RF silence. The protocol is practical from a deployment point of view and it not only meets the formal definitions of strong privacy and untraceability, but also addresses most, of the concerns raised by privacy advocates on behalf of consumers. Both passive and active RFID systems can use this protocol, and with slight modifications it can also be used on wireless-sensor networks. The protocol is expected to more efficiently utilize the RF spectrum by minimizing tag and reader collisions and as a result it should be possible to accommodate more readers and tags in a given area.**

***Index Terms*—RFID, wireless-sensor networks, privacy, zero-knowledge protocols, RF silence, collision avoidance**

I. Introduction

Radio Frequency Identification (RFID) promises to be an important enabling technology for concepts, such as the Internet of Things, where tagged physical objects are accessed and monitored from cyberspace. Of particular interest are RFID systems using passive tags (transponders), because they allow for miniaturization and do not require in-field maintenance. Several obstacles are standing in the way of RFID technology fulfilling this promise. Foremost, among these obstacles is the general public's concern regarding the lack of security and privacy protections in today's passive RFID systems. In this paper we seek to address the question of RFID security and privacy by proposing a practical and flexible solution that we believe addresses most, if not all, of the general public's concerns, while at the same time satisfying the generally accepted technical requirements for secure, privacy preserving RFID systems.

The protocol we propose is best viewed as a hierarchically layered set of services. It offers security by encrypting all communication between devices. Privacy is preserved firstly, by having all devices in the system only respond to authenticated messages, and secondly, any responses are indistinguishable from random messages. The protocol has the following features:

1) All communications between the reader and the tag are local, no global database is required in the backend to authenticate messages, and so an unlimited number of readers and tags can be added to the system without compromising the availability, security and performance of a global database.
2) The protocol can be used in both active and passive RFID systems.
3) Reader and tag commands (opcodes) in the protocol can be easily extended to give the system more functionality. For example, tag commands can be added to enable tags to act as interfaces between wireless sensors on a tagged item and the network monitoring these sensors.
4) The protocol has an option to turn off the security and privacy-preserving features and so allowing for protocol extensions that are backward-compatible with today's insecure protocols for passive RFID systems.

The rest of the paper is organized as follows. Section II looks at some related work. In Section III we examine the notion of privacy and propose a working definition of privacy that we believe is very broad and can be used in developing a privacy-preserving RFID protocol. Next we discuss the assumptions and design principles that we adhered to in the development of the protocol. In section IV we present the details of our protocol, beginning with the protocol layers and describing the principal algorithms, and then presenting the full protocol. In section V we analyze the protocol using a formal model and show that devices using this protocol are untraceable. We also look at anti-collision systems and scalability in relation to our protocol. We conclude the paper in Section VI.

II. Related Work

In recent years there has been a significant increase in research focused on RFID security and privacy, as evidenced by the number of papers published on the subject [1]. Juels presented a comprehensive survey covering most of the mainstream research initiatives on RFID security [2]. Avoine in [3] defined the notions of existential and universal untraceability in a very general and flexible way; he then went on to propose formalism for traceability. This formalism allows for a rigorous analysis of the privacy-preserving or untraceability features of RFID protocols. Juels and Weis proposed a simpler, but less flexible definition of RFID privacy; they then used this definition to highlight the vulnerabilities in some proposed privacy-preserving protocols [4].

Engberg *et al*. proposed a "zero-knowledge" RFID security and privacy protocol [5], where the tag only responds to authenticated readers. However, Engberg *et al*. did not provide sufficient details on how their protocol works and on how the shared secret keys were managed, in order to

Manuscript received November 16, 2012; revised January 17, 2013.

C. Mutigwe is with the School of Electrical and Computer Systems Engineering, Central University of Technology, Bloemfontein, South Africa (e-mail: cmutigwe@ ieee.org).

F. Aghdasi is with the Faculty of Science and Agriculture, University of Fort Hare, Alice, South Africa (e-mail: faghdasi@ufh.ac.za).

J. Kinyua is with the School of Computer Information Systems, Virginia International University, Fairfax, VA 22030 USA (e-mail: jkinyua@viu.edu).

enable their model to be subjected to a detailed formal analysis. The vulnerabilities within the Engberg et al. protocol are outlined in [2] and [4]. RFID security protocols can be classified as online or offline. Online protocols require a global database networked to the reader(s) for tags to be authenticated, while offline protocols have no need for such a database. Our protocol is an offline protocol and it is similar to that of Engberg *et al*. however; it addresses all the vulnerabilities mentioned in [2] and [4]. Furthermore, of the four stages in RFID tag lifecycle [5]; (1) supply chain management, (2) in-store and point-of-sale (POS), (3) customer control and aftersales servicing, and (4) recycling and waste management, the Engberg *et al*. protocol only addresses stages (2) and (3), while our protocol addresses all the lifecycle stages.

Avoine and Oeschslin demonstrated that RFID privacy cannot be viewed as an application layer problem only, but should be addressed as a multi-layer problem [6], and this is our approach in this paper.

III. Privacy and Security in a Wireless Environment

Today's passive RFID systems, like the original versions of the World Wide Web, were not designed with security and privacy in mind. With the Internet, individuals could choose not to use offending applications of the technology. However the fear with RFID technology is that when item-level tagging is more widely adopted consumers will not be presented with a choice. In this section we look at the question of privacy and then outline the positions we took in designing our protocol.

A. What is Privacy?

Protecting the privacy of persons or enterprises in possession of RFID tagged items requires that we have a common interpretation of what we mean by the concept of privacy. At the personal level, the notion of privacy can best be captured by studying the answers that an individual gives when presented with a situation in which they are a participant and are then asked to create a list of persons who should not have any knowledge about them in that situation [7]. Based on these lists we come to the conclusion that the notion of privacy is contextual. Furthermore, if this exercise were conducted in different parts of the world we would find that this notion is defined differently in other cultures and thus privacy is protected differently by the legal structures in those societies [8]. Solove [9] discusses several other conceptions of privacy and highlights the shortcomings in each one.

A related concept that is of particular concern to the RFID privacy discussion is that of 'privacy in public', which deals with the issue of whether individuals can expect privacy when they knowingly or unknowingly expose information about themselves in public spaces. An example of this is illustrated by a scenario where all the items in a store are tagged with an EPCglobal Class 1 tags and a shopper purchases some items and the tags on the purchased items are not de-activated. When the purchaser leaves the store and walks in the public areas, should they expect privacy regarding their purchases given the fact that the tags on the items will respond to any interrogator operating at the appropriate frequency? Courts in the United States have tended to take the view that there can be no "reasonable expectation of privacy" with regards to information that one exposes in a public area [10].

Now, those wishing to develop privacy-preserving RFID solutions are presented with the challenge of protecting an ill-defined concept, but one that is very real to prospective end-users. The best solution is one that takes the broadest view of this concept; unfortunately this will most likely be the most costly option, in terms of direct costs. In this paper we take the broadest view of this concept and attempt to define privacy as the freedom from unlicensed observation of and interference with one's personal space. This personal space consists of: (a) the physical, emotional or spiritual state of the individual, (b) any records held by other parties describing or identifying the individual, and (c) the individual's relationships and transactions with other parties. Given the levels of current concerns about privacy in RFID systems, we are of the opinion that the direct costs incurred by adopting the broadest view will be offset by the increased trust from end-users and wider market access for these more trusted systems.

B. Design Principles

The following principles form the foundation of our protocol.

Anonymity: Privacy in an RFID communication channel can be preserved by ensuring that each message exchanged between the tag and the reader appears as a random encrypted message to any eavesdropper. In this way the reader and tag cannot be identified based on the messages that they exchange; that is they are anonymous. This process of anonymizing can be achieved by having the transmitting party, for each outgoing message; generate a *nonce*, append the *nonce* to the message, encrypt the message, and then transmit the encrypted message. This guarantees that the messages sent out by the transmitting party are random, and satisfies Juels and Weis' definition of strong privacy [4]. The receiving party decrypts the messages using a shared key, in the case of systems using symmetric key cryptography, and then extracts the original message.

Juels and Weis' definition of strong privacy [4] and Avione's definition of ' untraceability' (*Universal-UNT*) [3] both assume that multiple entities are transporting tagged items. In those circumstances where a single entity is transporting a tagged item, then the notion of preserving privacy through anonymity fails to hold, for in this case the entity can be tracked using its un-decrypted responses to reader queries. Furthermore, using a network of two or more readers the entity's exact location can be determined by triangulation.

In our protocol each transmitting unit will act as an anonymizing agent by employing the techniques outlined above, however we have added features to help deal with the limitations discussed above.

RF Silence: Communication in our protocol will be initiated by the reader. The tags will only respond to authenticated readers, while the readers will acknowledge or respond only to authenticated tags. As outlined in the section

on anonymity, each message from the reader or tag is anonymized and encrypted using a shared secret key to secure the communications.

Maintaining RF silence to any un-authenticated inquiry, addresses the limitation with the anonymizing-only protocols when only one tagged item is present in a given environment or a single person at a given location has tagged items. Communicating only with authenticated readers, allows for addressable communication between the reader and the tag, using a ReaderID and a TagID, once a secure channel has been established. An equally important advantage of our protocol is that it will allow the RF spectrum to be utilized more efficiently, by minimizing random broadcasts by tags.

Engberg *et al*. [5] proposed a protocol that was similar to this one, however their anonymizing process was dependent on a timestamp and as outlined by Juels and Weis [4] this creates vulnerability with this protocol. Our protocol is not dependent on any timestamps for authentication or anonymizing. Although it is not detailed in our protocol, its implementation can include power analysis countermeasures, to ensure that silence at the logical layer is translated to RF silence. This latter requirement will address the second concern that Juels and Weis raised with the Engberg *et al*. protocol [4].

The key management mechanism used to assign and transfer the shared keys will be outlined in the Tag Ownership and Transfer section. In our protocol we have allowed for the capability to turn-off the RF silence capability through our key management mechanism for those environments where promiscuous tags and tree-based anti-collision algorithms are advantageous.

Tag Ownership and Transfer: In our protocol the entity or person that is in legal possession of the tagged item owns the secret key or PIN that a reader must have in order to be able to communicate with the tag. Before transferring a tagged item to a new owner, the current holder has the obligation of updating the PIN on the tag, using the protocol's PIN Update command, to a new unique PIN that will only be available to the new holder.

In a retail setting we envisage this key management mechanism being implemented in one of two ways at the Point-of-Sales (POS). The first option is for shoppers using cash for their purchases, when the item has been paid for, before it is bagged and/or handed back to the customer, the PIN on the tag is updated with the receipt number. Receipt numbers may also be encoded in a bar code to assist with the handling of returns or other home post-purchase RFID appliances. The second option is for those shoppers using swipe cards or wireless payments. In this case, the process is the same as in the first option, except that the receipt number will not be used. In this case part of the credit or debit card number will be used to generate the PIN. An example would be to construct the PIN using only the digits on the even positions in credit or debit card number. With this option at-home post-purchase RFID appliances only need to have their PIN entered once and for returns the consumer doesn't need to bring in a receipt, they just need to take the return item in together with the card that was used to make the purchase. Using the newly-launched NFC-enabled cards or mobile devices, such as the payWave card by Visa [11], payments and tag PIN updates can all be done wirelessly. These wireless PIN updates address a criticism of the of PIN-based RFID access control systems raised by Juels [2]. Consumers should be notified on the receipt or otherwise at the POS what the PIN for their purchases is.

In an enterprise setting the key management mechanism will be simpler; the initial PIN and the procedures for transmitting new PINs will all be setup at the launch of any partnerships.

An added advantage of this key management scheme is that a tag holder can transfer ownership of the tag to another party, while ensuring that past tag history remains private. The new tag owner can update the PIN as often as they wish if they have the means.

Invariance of Privacy Expectations: In the development of our protocol we adopted the principle that given two similar situations, where privacy is a concern and RFID technology is being used in one situation, while another technology is being used in the other, then RFID technology should not be expected to provide for more privacy that the other technology.

While every effort has been made in our protocol to address concerns raised by privacy advocates, such as the Privacy Rights Clearinghouse [12], the principle adopted above will at times be at variance with the positions taken by some privacy advocates. As an example, we consider the case of in-store tracking, where the Privacy Rights Clearinghouse takes the position that consumers in the store must consent to RFID tracking, however no such restrictions exist for in-store video surveillance, which when combined with image recognition software can be more revealing, or for the use of cookies and other tracking tools in online stores. In our protocol, the only way one can prevent tracking is if they own the tag and hence the PIN, in the case of in-store tracking the entity in legal possession of the tag is the store, that changes once the item is purchased and then the store can no longer track that item unless it is returned by the purchaser.

C. Assumptions

In developing the protocol we made the following assumptions:

Physical Security: We assumed that the tagged items were physically secure. Should the physical security be compromised then our protocol can no longer guarantee that privacy will be preserved going forward. For example, the attacker can attach a hidden tag to the item that operates at a non-standard frequency and thus track the tagged item. To help secure the PIN in the case of brute force attack, we have implemented a throttling feature in the protocol where the wait time before a new query is processed increases exponentially with each failed authentication query.

Secure Channels: The channel between the reader and the PIN capture system, labeled 1 in Fig. 1 can use a wired or wireless interface. We assumed that this channel is secure. The memory channel, labeled 4 in Fig. 1, is secure based on our protocol, and as we will show this channel can only be accessed by an authenticated reader. All the other channels were assumed to be insecure.

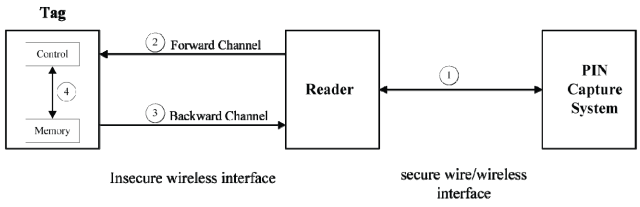

Fig. 1. Communication channels.

Security Model: In this paper we adopted as our security model Avoine's adversarial model [3]; it is in our view the most flexible RFID security model and most of the other models tended to be subsets of it.

IV. Protocol Details

Our proposed scheme at the top level can be viewed as a set of hierarchical layers. Details of these layers are presented below, along with the algorithms used to implement the core functions. An outline of the complete protocol is presented at the end of this section.

A. Protocol Layers

Our protocol is based on the three layer stack shown in Table I. Each layer interacts directly only with the layer immediately beneath it, and provides facilities for use by the layer immediately above it.

TABLE I: RFID Communication Protocol Layers

Layer	Function
1. Key Management	Tag ownership, PIN assignment and exchange
2. Security	Message randomizing, encryption and authentication
3. Communication	Tag commands, reader commands, and session management

Layer 1: The key management layer implements the tag ownership policy through the administration of the PIN or secret key (k_x) for each session (x). The PIN then determines which readers can communicate with the tag. Details of the key management mechanism were presented in the Tag Ownership and Transfer section.

Layer 2: The security layer ensures that each outgoing message has been made untraceable by generating a nonce (n_x) and embedding it in the message, to create a 'random' message (m_o).

Algorithm 1 $Message(ID, k_x, cmd, newKey)$

1. $n_x \leftarrow generate(nonce)$
2. $m_o \leftarrow (n_x, ID, newKey, cmd)$
3. $m_a \leftarrow MAC(m_o, k_x)$
4. $m_c \leftarrow (m_o, m_a)$
5. $m_e \leftarrow encrypt(m_c, k_x)$
6. **return** m_e

A Message Authentication Code (MAC) of the 'random' message (m_a) is generated using the PIN from the key management layer. The algorithm for the *Message* function, which randomizes and encrypts the outgoing message, is outlined in Algorithm 1. The *cmd* and *newKey* inputs are optional and they are used to transmit, as part of the outgoing message, a command or a new key, respectively. (k_x) ID represents the identifier of the tag or the reader, depending on the message source.

The receiver first checks to determine if the security feature is turned on and if it is, the incoming message is checked against a set of recently received protocol initiation messages, if the message is a duplicate (potential replay attack), it is discarded and the throttling function is called, else the message is decrypted and then the 'random' message and MAC are extracted. The receiver then generates the MAC of the 'random' message, using its PIN and compares its MAC to the extracted MAC. Details of the authentication process are shown in Algorithm 2.

Algorithm 2 $Authenticate(m, k_j, j)$

// Security turned off for backward compatibility
1. **if** $k_j = k_{off}$ **then**
2. $tree{-}based\ anti{-}collision(m)$
3. $m_o \leftarrow extract(m, message)$
4. **return** 1 // Authentication successful
5. **end if**

// For all other authentication requests
6. **if** $m \in \{recent\ protocol\ initiation\}$ **then**
7. $wait(T^j)$ // Exponential throttling
8. **return** 0
9. **end if**
10. $m_o^{j'} \leftarrow extract(decrypt(m, k_j), message)$
11. $m_a^{j'} \leftarrow extract(decrypt(m, k_j), mac)$
12. $m_a^{\omega} \leftarrow MAC(m_o^{j'}, k_j)$
13. **if** $m_a^{j'} = m_a^{\omega}$ **then**
14. **return** 1
15. **else**
16. $wait(T^j)$
17. **return** 0
18. **end if**

Layer 3: The communication layer manages the session between the reader and the tag. Tags can only engage in one session at a time, while readers can be engaged in multiple sessions simultaneously. Reader-tag communication is addressable, that is, for each session the tag knows which reader (based on the reader ID) it is communicating with and similarly the reader knows which tag (based on the tag ID) it is communicating with. The message received from the security layer is parsed and (a) the transmitter's ID is used to determine whether this is a response from a valid transmitter or not (b) if the transmitter is valid, the command to be performed is extracted and tested to determine if it is a valid command given the status of the session, Table II shows the list of commands. For wireless sensor networks additional reader and tag commands may be added to the list shown in Table II, to allow the tag to act as an interface between the reader and the sensor.

Session management algorithms for the tag and reader are presented in Algorithm 3 and Algorithm 4, respectively.

Algorithm 3 $TagSession(m)$

```
1.  ReaderID ← extract(m, ID)
2.  opcode ← extract(m, cmd)
    // ALOHA slot info in ID
3.  time ← RND(extract(m, slot(ID)))
4.  if (opcode = R_init) and (session = 0) then
5.     rID ← ReaderID
6.     session ← 1
7.     return TagID
8.  else if rID ≠ ReaderID then
9.     return 0 // Reader not valid for this session
10. end if
11. if (opcode = R_ae) and (session = 1) then
12.    return 1
13. else if (opcode = R_au) and (session = 1) then
14.    k_j ← extract(m, key)
15.    return 1
16. else if (t > t_0 + time) and (session = 1) then
17.    k_j ← extract(m, key)
18.    return 2 // Retransmit, possible collision
19. else
20.    return 0
21. end if
```

TABLE II: READER COMMANDS

Command	Description
R_{init}	Protocol initiation with reader ID
R_{ae}	Reader acknowledgment & end session
R_{au}	Reader acknowledgment & PIN update

V. DISCUSSION

A. Complete Communication Protocol

Let i and j denote the number of the protocol session and number of the authentication session for the reader, respectively. Similarly, let s and t denote the number of the protocol session and number of the authentication session for the tag, respectively. Let n_{ij} be the *nonce* for the outbound message from the reader and k_i be the reader's secret key (PIN) for the protocol session. An outline of how all the core functions of the protocol are related is presented in Fig. 2.

Algorithm 4 $ReaderSession(m)$

```
1.  TagID ← extract(m, ID)
2.  if tID is NULL then
3.     tID ← TagID
4.     session ← 1
5.  else if tID ≠ TagID then
6.     return 0 // Tag not valid for this session
7.  end if
8.  if update_tag_key = yes then
9.     session ← 0
10.    return new key
11. else
12.    session ← 0
13.    return 1
14. end if
```

In this section we formally analyze the protocol and also highlight its anti-collision and scalability features.

B. Analysis

Here we will demonstrate that our protocol is both privacy-preserving and secure, except in those circumstances where the tag owner sets its PIN to k_{off}. This exception was provided to enable RFID systems using our protocol to be backward-compatible with systems that have no security, such as today's RFID systems that use EPC Class 1 tags.

We will analyze our protocol using Avoine's adversarial model [3]. In this model, the attacker is represented by an adversary $\mathcal{A}$ and the RFID system is represented by a *Challenger*. The tag $\mathcal{T}$ and the reader $\mathcal{R}$ can each run several instances of the RFID protocol $\mathcal{P}$. We define an interaction $\mathcal{I}$ as a set of executions on the same tag at a time when A is in a position to physically identify it. $\mathcal{A}$ has as means the *Query*, *Send*, *Execute*, *Execute**, and ***Reveal*** oracles, denoted by Q, S, E, E^*, and R, respectively. Avoine defines the notion of untraceability (*UNT*) as follows:

Existential Untraceability

Parameters: l_{ref}, l_{chal}, $\mathcal{O} \subset \{Q, S, E, E^*, R\}$.

1) $\mathcal{A}$ requests the *Challenger*, she in response receives her target $\mathcal{T}$.
2) $\mathcal{A}$ chooses $\mathcal{I}$ and calls $Oracle(\mathcal{T}, \mathcal{I}, \mathcal{O})$ where $|\mathcal{I}| \le l_{ref}$ then receives $\hat{\Omega}_{\mathcal{I}}(\mathcal{T})$.
3) $\mathcal{A}$ requests the *Challenger* thus receiving her challenge $\mathcal{T}_1$ and $\mathcal{T}_2$, and $\mathcal{T} \in \{\mathcal{T}_1, \mathcal{T}_2\}$.
4) $\mathcal{A}$ chooses $\mathcal{I}_1$ and $\mathcal{I}_2$ such that $|\mathcal{I}_1| \le l_{chal}$, $|\mathcal{I}_2| \le l_{chal}$, and $(\mathcal{I}_1 \cup \mathcal{I}_2) \cap \mathcal{I} = \varnothing$.
5) $\mathcal{A}$ calls $Oracle(\mathcal{T}_1, \mathcal{I}_1, \mathcal{O})$ and $Oracle(\mathcal{T}_2, \mathcal{I}_2, \mathcal{O})$ then receives $\hat{\Omega}_{\mathcal{I}_1}(\mathcal{T}_1)$ and $\hat{\Omega}_{\mathcal{I}_2}(\mathcal{T}_2)$.
6) $\mathcal{A}$ decides which of $\mathcal{T}_1$ or $\mathcal{T}_2$ is $\mathcal{T}$, then outputs her guess $\mathcal{T}'$.

Universal Untraceability

Parameters: l_{ref}, l_{chal}, $\mathcal{O} \subset \{Q, S, E, E^*, R\}$.

1) $\mathcal{A}$ requests the *Challenger*, she in response receives her target $\mathcal{T}$.
2) $\mathcal{A}$ chooses $\mathcal{I}$ and calls $Oracle(\mathcal{T}, \mathcal{I}, \mathcal{O})$ where $|\mathcal{I}| \le l_{ref}$ then receives $\hat{\Omega}_{\mathcal{I}}(\mathcal{T})$.
3) $\mathcal{A}$ requests the *Challenger* thus receiving her challenge $\mathcal{T}_1$ and $\mathcal{T}_2$, $\mathcal{I}_1$ and $\mathcal{I}_2$.
4) $\mathcal{A}$ calls $Oracle(\mathcal{T}_1, \mathcal{I}_1, \mathcal{O})$ and $Oracle(\mathcal{T}_2, \mathcal{I}_2, \mathcal{O})$ then receives $\hat{\Omega}_{\mathcal{I}_1}(\mathcal{T}_1)$ and $\hat{\Omega}_{\mathcal{I}_2}(\mathcal{T}_2)$.
5) $\mathcal{A}$ decides which of $\mathcal{T}_1$ or $\mathcal{T}_2$ is $\mathcal{T}$, then outputs her guess $\mathcal{T}'$.

The advantage of $\mathcal{A}$ for a given protocol $\mathcal{P}$ is defined by:

$$Adv_{\mathcal{P}}^{UNT}(\mathcal{A}) = 2Pr(\mathcal{T}' = \mathcal{T}) - 1$$

where the probability space is over all the random tags. If $\mathcal{A}$'s advantage is negligible with the parameters l_{ref}, l_{chal} and $\mathcal{O}$, then $\mathcal{P}$ is said to be $UNT_{l_{ref},l_{chal}}$–$\mathcal{O}$ secure, usually simply denoted by UNT–$\mathcal{O}$.

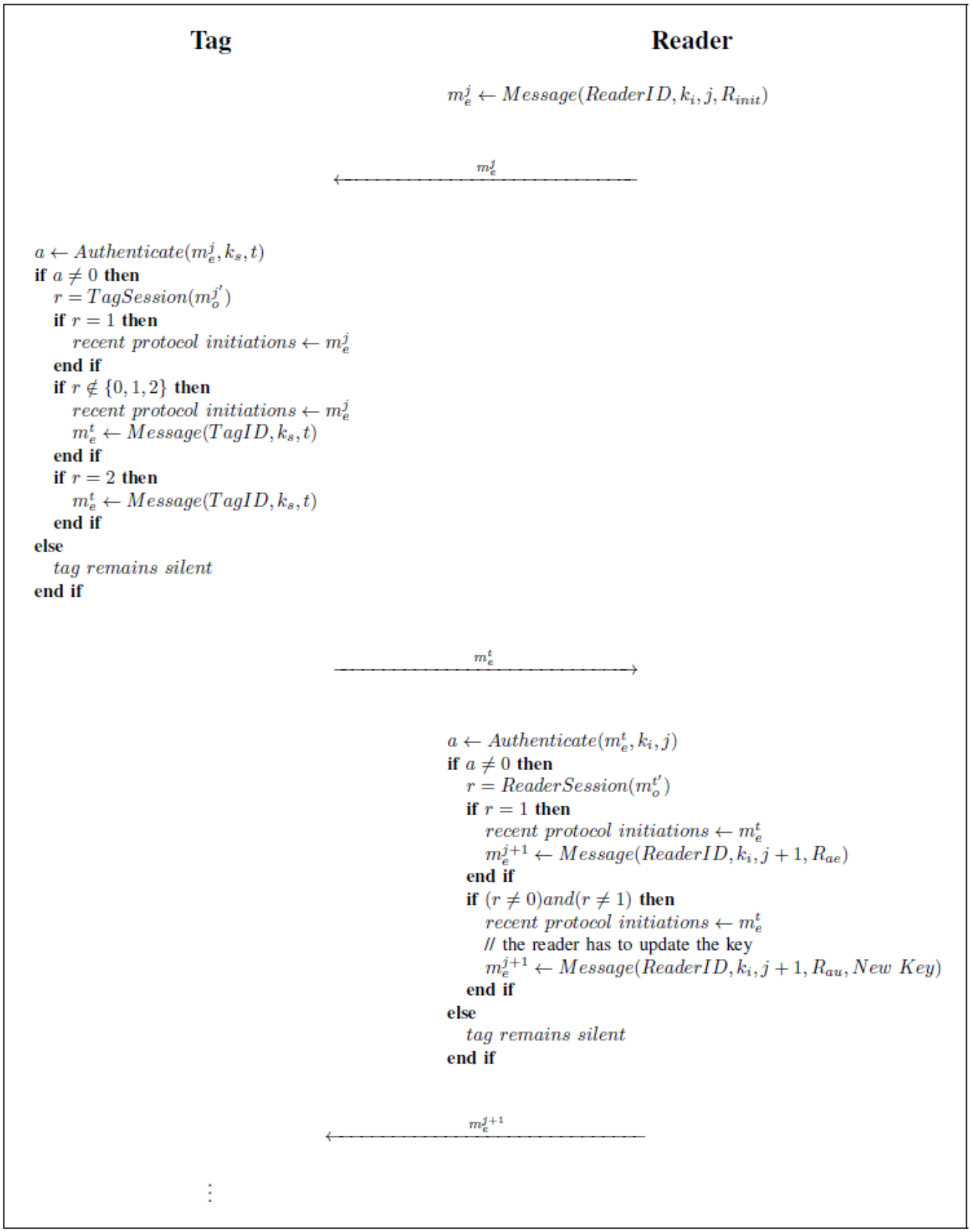

Fig. 2. The RFID communication protocol. Arrows represent wireless message transmissions.

Below we show that our protocol is *Existential-UNT-QSE*, implying that it is *Universal-UNT-QSE*. We also show that it is *Universal-UNT-R*, implying that it is *Universal-UNT-QSER*.

In our protocol the information sent by the tags and the readers gives no useful information to an attacker, since they cannot distinguish it from any random numbers. In step 5 of the Existential Untraceability experiment, due to RF silence

for unauthenticated messages, $\hat{\Omega}_{\mathcal{T}_1}(\mathcal{T}_1) = \hat{\Omega}_{\mathcal{T}_2}(\mathcal{T}_2)$, therefore $\mathcal{T}$ is a guess between two equally likely alternatives and $Pr(\mathcal{T}' = \mathcal{T}) = \frac{1}{2}$. Consequently, our protocol is *Existential-UNT-QSE*. The protocol by managing each session between $\mathcal{T}$ and $\mathcal{R}$, and storing recent successful protocol initiation queries is also resistant to replay and "man-in-the-middle" attacks.

Now *Existential-UNT-QSE* → *Universal-UNT-QSE* and if an attacker tampers with the tags and obtains its PIN, i.e. uses the Reveal oracle, our protocol through the key management mechanism will not allow the attacker to track all the past events of the tag, meaning that our protocol is *Universal-UNT-R*. Since the protocol is *Universal-UNT-QSE* and *Universal-UNT-R*, therefore the protocol is *Universal-UNT-QSER*.

A. Collisions

For tag anti-collision our protocol uses a modified version of the slotted ALOHA protocol [13]. It is expected that our protocol will result in fewer tag collisions, since there will be less traffic on the forward and backward channels shown in Fig. 1. Tags and readers will only respond to transmitters with the same PIN, and even in those circumstances where there are multiple readers with the same PIN at a given location, once a tag establishes a session with a reader it will only communicate with that reader and will not respond to other readers even though they share the same PIN.

Multiple readers at a given location can be setup to query tags in a round-robin fashion in order eliminate reader collisions and to increase the read throughput of tags.

B. Scalability

Online protocols generally suffer from the problem that they do not scale well as the RFID system grows because:

1) The computational resources, including network bandwidth, needed by the backend database grows as the number of readers and tags in the system grows.
2) A single, central database is required to track the tags from manufacture to disposal and this does not allow for disparate users and systems to use the RFID application in a flexible way. Users are presented with an "all or nothing" proposition.
3) The availability of the database presents a single point of failure, if the database is unavailable for whatever reason, then the entire system fails.

In our protocol each reader, key-capture device, and set of tags constitutes a stand-alone secure, privacy-preserving RFID system that does not need a backend database and so can be deployed in an ad-hoc fashion.

Furthermore, items tagged using our protocol do not assume that the end-user will use the tags in their system. End-users are presented with the option to use the tags if they have the infrastructure, and if not the tags will remain silent and thus not expose them to unsolicited risks, as some tagged items currently do.

VI. Conclusion

A discussion on the conceptions of privacy was presented and from this discussion a working definition of privacy was developed. Based on the privacy definition, the design goals and assumptions for the proposed protocol were then presented. A zero-knowledge-based communication protocol for RFID systems was then developed. The primary feature of the protocol is that tags only responding to authenticated readers, otherwise tags always maintain RF silence.

A potential avenue for future research is to explore the relationship between the end-users cultural or contextual privacy preferences and the rate of RFID technology adoption. Another avenue is to conduct experiments to test the assertion that our proposed protocol will utilize the RF spectrum more efficiently than existing broadcast RFID protocols, due to the addressable nature of communications in our protocol.

References

[1] RFID security and privacy lounge. (November 2012). Universit Catholique de Louvain, Information Security Group. [Online]. Available: https://www.privacyrights.org/ar/RFIDposition.htm

[2] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[3] G. Avoine, "Adversary model for radio frequency identification," *Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC)*, Lausanne, Switzerland, Technical Report LASECREPORT- 2005-001, Sep. 2005.

[4] A. Juels and S. Weis, "Defining strong privacy for RFID," in *Proc. International Conf. on Pervasive Computing and Communications (PerCom'07)*, New York, USA, March 2007, pp. 342-347.

[5] S. Engberg, M. Harning, and C. D. Jensen, "Zero-knowledge device authentication: privacy & security enhanced RFID preserving business value and consumer convenience," in *Proc. Conf. on Privacy, Security and Trust (PST'04)*, New Brunswick, Canada, October 2004, pp. 89-101.

[6] G. Avoine and P. Oechslin, "RFID traceability: a multilayer problem," in *Proc. Conf. on Financial Cryptography (FC'05), ser. Lecture Notes in Computer Science*, A. Patrick and M. Yung, Eds., Roseau, The Commonwealth Of Dominica: Springer, February– March 2005, vol. 3570, pp. 125-140.

[7] A. P. Bates, "Privacy-a useful concept?" *Social Forces*, vol. 42, no. 4, pp. 429-434, 1964.

[8] B. Moore, *Privacy: Studies in Social and Cultural History*, New York: M. E. Sharpe, 1984.

[9] D. Solove, "Conceptualizing privacy," *California Law Review*, vol. 90, no. 4, pp. 1087-1155, 2002.

[10] H. Nissenbaum, "Protecting privacy in an information age: the problem of privacy in public," *Law and Philosophy*, vol. 17, no. 5/6, pp. 559-596, 1998.

[11] Visa payWave. (November 2012). Visa, Inc. [Online]. Available: http://usa.visa.com/personal/cards/card technology/paywave.html

[12] RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. Privacy Rights Clearinghouse. (November 2003). [Online]. Available: https://www.privacyrights.org/ar/RFIDposition.htm

[13] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. New York: John Wiley and Sons, 2003.

Charles Mutigwe was born in Zimbabwe in 1970. He obtained a bachelor's degree in electrical engineering from the University of Zimbabwe, Harare, Zimbabwe in 1994; a master's degree in electrical engineering from Western New England University, Springfield, Massachusetts, U.S.A. in 2003; and an M.B.A. from Norwich University, Northfield, Vermont, U.S.A. in 2005. He is a doctoral candidate in electrical engineering at the Central University of Technology, Bloemfontein, South Africa.

He is currently an IT & Data Analyst at the University of Massachusetts (UMass) Amherst. He is also an adjunct professor at the Isenberg School of Management at UMass Amherst, where he teaches Information Management

in the online MBA program. He has worked as an IT professional for over 15 years and his previous positions include: Systems Engineer, Systems Administrator, Systems Developer, Lab Manager and IT Director at dot-com start-ups, a university and Fortune500 companies. His research interests are: electronic design automation, reconfigurable computing and RFID systems.

Mr. Mutigwe is a member of the IEEE, the IEEE Computer Society and the ACM.

Farhad Aghdasi obtained a bachelor's degree with honors in electronic & electrical engineering from the University of Manchester, in the U.K.; a master's degree in electrical & computer systems engineering from Oregon State University, Corvallis, Oregon, U.S.A.; an M.B.A. degree from the University of Portland, Oregon, U.S.A.; and a PhD in Electrical Engineering from the University of Bristol, in the U.K.

He is currently the Dean of the Faculty of Science and Agriculture at the University of Fort Hare in South Africa. Over the past 30 years he has held academic posts in universities in Southern Africa including Professor and Director: School of Electrical and Computer Systems Engineering and Dean of the Faculty of Engineering and Information Technology, Central University of Technology, Bloemfontein, South Africa; Vice-Rector: Academic Affairs and Research, Polytechnic of Namibia, Windhoek, Namibia.

Prof. Aghdasi is currently the NRF grant holder for the Risk and Vulnerability Assessment Centre (RAVAC) for food and water security in the Eastern Cape region of South Africa. Prof. Aghdasi's passion is to increasingly use the postgraduate research projects and postdoctoral activities for innovations in the betterment of the lives of the community, job creation, collaboration with the industry and adding quality to teaching and learning of undergraduates.

Johnson Kinyua was born in Kenya in 1958. He obtained a bachelor's degree in electrical engineering from University College London (UCL), London in United Kingdom (U.K.) in 1981; a master's degree in digital communications from the University of Kent, Canterbury in U.K. in 1984; and a PhD in computer science from the University of Cambridge, Cambridge in U.K. in 1992.

He is currently the Dean and Professor in the School of Computer Information Systems at Virginia International University, Fairfax, VA, USA. He has publishes widely in international journals and conferences. His previous positions include: Research & Innovation Professor, Associate Professor and Director, Senior Lecturer and Lecturer at different universities. His current and previous research interests are: Software Engineering, Cybersecurity, Database Security, Security Engineering, Distributed Systems, multi-agent systems, Fixed and Wireless networks, and Computer Architecture.

Prof. Kinyua is a member of the IEEE, the IEEE Computer Society and the ACM. Prof. Kinyua has acted as an external examiner for several universities, has been a panel member for external program assessment of programs at two universities and was a committee member of the higher education qualifications accreditation committee in South Africa for a number of years. Prof. Kinyua is member of the international technical program committees (TPC) for two international conferences: ITNG networking track (see http://www.symbolicscience.com/ITNG2012.pdf), held annually in Las Vegas; and IASTED African Conference on Modeling and Simulation (http://www.iasted.org/conferences/ipc-685.html).