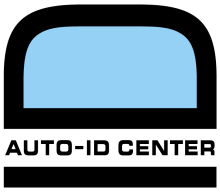
Published October 1, 2003. Distribution restricted to Sponsors until January 1, 2004.



TECHNICAL REPORT

Micronetwork Interfaces for RFID Tags: A New Paradigm for Reader-Tag Communication

Daniel W. Engels

AUTO-ID CENTER MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 400 TECHNOLOGY SQ, BUILDING NE46, 6TH FLOOR, CAMBRIDGE, MA 02139-4307, USA

ABSTRACT

We present a new, standardized network communication oriented approach to Radio Frequency Identification protocol design. As RFID systems become ubiquitous and used in a plethora of distinct applications, the functionality that may be contained within the RFID tags will become extremely varied. RFID tags are typically implemented as small embedded systems consisting of one, or a very few, microchips. Ubiquity will bring standardization of the communication interfaces, enabling multiple manufacturers to produce tags with the same interfaces and possibly different functionality or produce a single component implementing specific functionality that is integrated with the tags from multiple vendors. Access to the functionality on the tag has traditionally been accomplished through the use of specific command codes issued by the reader, utilizing a design philosophy similar to that taken in microprocessor and co-processor command set design. The extreme variation in functionality that may be implemented within the ubiquitous standardized tags precludes the use of the traditional command code method of accessing on-tag functionality. We present a standardized network communication oriented method for accessing on-tag functionality. This method views the on-tag functionality as separate components connected via a **micronetwork** and communicated with through a **micronetwork gateway**. Similarly, the reader-tag communication channel is viewed as a **wireless micronetwork** connecting the reader with its functional components, the tags in its interrogation zone, and the reader is the **micronetwork gateway** to the local network. This network oriented interface is tag functionality and implementation independent and seamlessly enables the implementation of new tag functionality without prior standardization.

Published October 1, 2003. Distribution restricted to Sponsors until January 1, 2004.

TECHNICAL REPORT

Micronetwork Interfaces for RFID Tags: A New Paradigm for Reader-Tag Communication

Biography

Daniel W. Engels
Director of Protocols

Daniel W. Engels received his B.S. from the University of Buffalo, his M.S. from the University of California, Berkeley, and his Ph.D. from the Massachusetts Institute of Technology all in Electrical Engineering and Computer Science. His master's thesis is in the area of computer-aided design for electronic systems, and his doctoral thesis is in the field of theoretical computer science. Dr. Engels joined the Auto-ID Center after obtaining his doctoral degree where he leads the day-to-day research activities of the Center. Dr. Engels' research interests include scheduling theory and applications, real-time system design, distributed and mobile computing, and computer-aided design for embedded systems.

TECHNICAL REPORT

Micronetwork Interfaces for RFID Tags: A New Paradigm for Reader-Tag Communication

Contents

1. INTRODUCTION

Radio Frequency Identification (RFID) systems are increasingly being used in a variety of diverse applications ranging from access control to supply chain management to remote sensing for quality control and beyond. Many of these applications can either benefit from or require specific on-tag functionality, such as an on-tag temperature sensor or password protected memory. The number of distinct on-tag functionality requirements is limited only by the number of distinct applications to which RFID systems are applied.

The most common approach to accessing all functionality on a tag is to use a unique command code for each function implemented on the tag and require an immediate response from the tag when the reader invokes a command [10][9][11]. This command-response, or **discrete command**, approach is similar to that taken in microprocessor design, with one command code allocated for each function that might be performed. From the perspective of the RFID tag reader, the tag appears to be a simple slave microprocessor (a co-processor if you will) that simply executes given commands and returns the result. Allocated command codes delineate the distinct functions that may be implemented by a tag, while the actual functions implemented by a specific tag can be a subset of the defined functions.

Co-processor-oriented functionality limits the allowable on-tag functionality to that which is amenable to discrete commands. Functionality such as encryption and security does not readily lend itself to discrete commands. This type of functionality is often on-going, or continuous. In other words, the functionality is executed continuously over a period of time. These functions are similar to daemons or other long running monitor processes. Continuous functions require **continuous commands** to begin and end their execution.

Furthermore, tags implementing high-complexity functionality, such as an on-tag microprocessor, are small embedded systems that may be executing user programmable functionality. The functionality implemented in software is limited only by the user, and the communication protocols with software processes may be user defined. A co-processor-based approach to accessing this highly varied functionality is at best difficult to implement and manage.

Managing a discrete and continuous command space is difficult within a standardized command environment. A single command space is easily managed when one RFID tag manufacturer, or a very small number of manufacturers, control the allocation of command codes to functionality. However, the potentially large number of RFID tag manufacturers operating within a standardized RFID framework complicates the command allocation process. The history of standardization efforts has shown that agreement on the allocation of functionality to command codes is often achieved only after an overly long discussion period. Delays to obtain standardization agreement limit the ability of individual manufacturers to provide market demanded functionality in a timely manner within the ubiquitous standard tag framework. These delays limit the usefulness of the standard and ultimately encourage the use of non-standard technologies.

As the potential on-tag functionality and capabilities increase, the co-processor based approach to command set design becomes untenable for standardized RFID systems. Therefore, a new approach must be pursued.

We propose a new **network oriented** approach to accessing on-tag functionality. We view a tag as a subnetwork containing possibly multiple computing devices that are all accessed through a single gateway to that network. In the network oriented approach, the tag interface is designed such that the tag appears to be a network gateway to additional devices implementing either application specific or general functionality. All functionality is accessed through a packet-based communication protocol between the reader and the tags. Only the resource discovery and communication protocols are standardized.

The implemented functionality and the manner to invoke that functionality within the standardized communication protocol are determined by the manufacturer of the tag. The amount of standardized tag functionality required to implement a tag to the standard is minimized in this approach. Furthermore, this approach provides for great exibility in the functionality that standardized tags may implement and provides for easy integration of components from multiple vendors. No multi-vendor agreements are required prior to the implementation of some new functionality, thus enabling manufacturers to quickly meet market demanded functionality.

The remainder of this paper presents our network oriented communication approach and is organized as follows. We provide an overview of RFID systems in Section II. Since tags are small embedded systems, Section III describes embedded systems and their use of micronetworks for component communication. Section IV describes the requirements for the use of a micronetwork. We note that an RFID tag is an embedded system with its components connected by an application specific micronetwork, and we note that an RFID system is an embedded system with the reader and the tags (the system components) connected via a wireless micronetwork. Section V describes our view of micronetworks within an RFID system and presents our micronetwork communication interface for RFID tags. Finally, Section VI draws the relevant conclusions.

2. OVERVIEW OF RFID SYSTEMS

This section provides a basic overview of RFID systems. We begin by reviewing the basic components that comprise RFID systems. We then review the basic operation of these components and brie y discuss application requirements on the system performance and functionality. Detailed descriptions of RFID systems may be found in [8] and [21].

2.1. System Components

All RFID systems are designed to automatically identify objects. This basic functionality leads to the use of three main components:

- the RFID tag, or **transponder**, which is located on the object to be identified,
- the RFID tag reader, or **transceiver**, which communicates with the tag to obtain information from it, and
- the **application subsystem** which utilizes the data and information obtained from the tags in some useful manner.

Typical RFID tags consist of an electronic microchip that stores data and executes the tag's functionality and a coupling element, such as a coiled antenna, used to communicate via radio frequency waves. Tags may have an on-tag power source, such as a battery or dedicated energy harvesting subsystem, to perform on-tag functionality. Tags without an on-tag power source must harvest their energy from the reader's communication signal and are unable to actively transmit a communication signal. Such tags are referred to as **passive tags**. Tags with an on-tag power source that do not actively transmit a communication signal are referred to as **semi-passive tags**, and tags that are capable of actively transmitting a communication signal are referred to **active tags**.

Typical RFID readers consist of a radio frequency module, a control unit, and a coupling element to wirelessly communicate with tags. In addition, readers are fitted with an interface that enables them to communicate with an application subsystem. The use of radio frequencies for communication with tags allows readers to communicate with passive RFID tags at short distances (typically less

than 10m), semi-passive RFID tags at medium distances (typically less than 100m), and active RFID tags at large distances (typically up to 1km) even when the electronic tags are located in a hostile environment and are obscured from view.

Application subsystems communicate with a set of readers and execute applications that utilize the data and information communicated to those readers from the tags in their communication zones.

2.2. System Operation

The basic components of an RFID system combine in essentially the same manner for all applications and variations of RFID systems. All objects to be sensed or monitored are physically tagged with transponders. The type of tag used and the functionality on the tag depends upon the application(s) to be executed by the application subsystem.

The applications executed by the application subsystem drive the required deployment and operation characteristics of the RFID tags and readers. The tags and readers simply provide the mechanism for gathering and communicating data and information regarding physical objects and their environments. Readers are strategically placed to communicate with tags where their data and information is required. For example, an RFID access control system locates its tag readers at the entry points to the secure area. A sports timing system, meanwhile, locates its readers at both the starting line and the finish line of the event.

The readers emit a communication signal whenever the application subsystem requires data and information from the tags in the reader's vicinity. The reader's communication signal forms a communication zone within which communication with tags is possible. The actual size of the communication zone is a function of the tag and reader characteristics, such as communication frequency and antenna size and polarity. Passive tags have the smallest communication zone since they must harvest energy directly from the reader's communication signal. Semi-passive and active tags are not power restricted in this way; thus, they typically have larger communication zones for a than an otherwise equivalent passive tag.

The application requirements determine the RFID system operation characteristics and on-tag functionality that are acceptable for that application. For example, an access control system requires a communication zone of a few inches (with a maximum communication zone extending only several inches). Thus, short communication range RFID systems must be used. Additionally, the access control system must use secure reader-tag communication protocols and secure the data and information stored on the tag to prevent tag communication with unauthorized readers.

3. EMBEDDED SYSTEMS AND MICRONETWORKS

Application specific electronic systems are typically referred to as **embedded systems**. Embedded systems are designed to execute a specific set of functionality that is often immutable over the life of the system. Small embedded systems provide integrated single-chip System on Chip (SoC) or small numbers of chips solutions to applications requiring potentially complex mixtures of functionality. Tight energy constraints characterize small embedded systems and wireless/mobile systems such as RFID tags. These systems are traditionally designed with highly integrated functionality to minimize both cost and power consumption. However, with the prevalence of complex system functionality and shortening design times these embedded systems are increasingly being designed by interconnecting existing general purpose and application specific components and custom application specific components [3][16][12][4][24].

An RFID tag is a small application specific, or embedded, system. We view an RFID tag as an embedded system that is a collection of loosely coupled components interconnected by a communication network. The interconnection network provides an efficient and convenient environment to access the distributed resources. Similarly, we view an RFID system as an embedded system that is a collection of wirelessly connected components (tags and readers) with the readers connected to an application subsystem. The wireless communication provides the interconnection network between the tag components and the reader components.

The trend towards complex embedded system functionality has led to embedded systems being micronetworks of networked components while the components themselves may be micronetworks of networked subcomponents. The **micronetwork** is an application specific local area network (LAN) and is used as the abstraction of the communication patterns among components. In a traditional LAN, communication with devices located on different networks occurs through a gateway. Similarly, the devices on a micronetwork communicate with devices located on different networks through a **micronetwork gateway**. Often, a single component only will act as a micronetwork gateway. In an RFID system, a tag's micronetwork gateway communicates with a reader, and a reader is a micronetwork gateway for the wireless micronetwork of tags in its interrogation zone.

Logically, a micronetwork operates in the same manner as a standard network. It is the communication channel used by distinct entities for communicating data and commands of interest. Micronetworks differ from traditional macronetworks such as LANs. These differences arise primarily because of differences in the design and performance constraints of the environments within which the different networks operate.

Communication network design has traditionally been decoupled from specific end applications and is strongly influenced by standardization and compatibility constraints in legacy network infrastructures. Application specific networks need only function sufficiently for the applications that utilize them. Consequently, macronetworks emphasize general purpose communications and modularity while micronetworks emphasize application specific communication and support specific communication patterns. Distributed embedded systems, such as wireless sensor networks, may combine both macronetwork communication for communication between distinct computing nodes and micronetwork communication for efficiency and exibility within a computing node.

The physical micronetwork is the physical instantiation of a system that enables these communication patterns to occur. In single-chip, or SoC, systems and small chip count systems, this physical micronetwork is limited by intrinsically unreliable signal transmission and significant communication delays along the communication medium connecting components. Synchronization of very large embedded systems with a single clock source and negligible skew will be extremely difficult, if not impossible for large SoC systems. In the absence of a single timing reference, embedded systems become distributed systems. Global control of the communication ows is unlikely to succeed because of the need to monitor each component's state. Thus, components will initiate data transfers autonomously, and the global communication pattern will be fully distributed.

The intrinsic variability in the application specific communication patterns enables multiple different physical micronetwork implementations. Regardless of the physical network implementation, the low-level data communication interface (and all higher level interfaces) to the components must be standardized to enable multiple vendors to manufacture components with the same functionality. Similarly, the physical networks must be standardized. A small set of standard physical networks, such as AMBA [17] and Core-Connect [14], will minimize the custom networks needed to interconnect components and enable plug-and-play networked component capabilities.

4. MICRONETWORKS

An RFID tag is an embedded system that is specifically designed to communicate with an external network, i.e., a reader, through a single micronetwork gateway. The various functional components and devices comprising an RFID tag are connected in an on-tag internal micronetwork. The micronetwork may have any one of a number of topologies such as a fully connected network or a star topology where the center of the star network is the micronetwork gateway. Since a micronetwork is a communication network, there are four basic issues that must be addressed in the micronetwork: naming and name resolution, routing strategies, connection strategies, and contention. The remainder of this section examines each of these issues with regard to the micronetworks in RFID systems.

4.1. Naming and Name Resolution

In order for two component nodes on a network to communicate with one another, they must be uniquely identified, or named, and they must know each other's unique identity. If host nodes can have more than one process executing simultaneously, then process identifiers must be used also to ensure that a node knows for which process a message is intended. The identifiers must conform to a standard for network communication such as an Internet Protocol (IP) address or an IEEE MAC address. In a micronetwork, the identifiers may conform to a non-scalable naming scheme since, by definition, the micronetwork connects a limited, and usually small, number of components. Therefore, eight (8) bit or smaller identifiers may be appropriate for some micronetworks.

Component nodes must either be preprogrammed with their communication partners' identifiers or must discover the identities of components with which they need to communicate (resource discovery). Resource discovery involves obtaining node identification, as well as identification of functional capabilities of each node. Within the RFID reader-tag micronetwork in an open RFID system, the reader identifies the tags via its tag-identification procedure. The resources available within a tag may be discovered either by querying the tag directly (if the tag has this information) once it has been identified or, if the identifier is a structured identifier such as an Electronic Product Code [1][2][5][6], the identifier may be used as a pointer to the tag's functionality description.

Within an RFID tag, either preprogrammed or dynamically allocated identifiers may be assigned to each functional component. Immutable identifiers, such as Media Access Control (MAC) identifiers [20], are typically preassigned at the time the device or component is manufactured. Mutable identifiers, such as Internet Protocol (IP) addresses [15][13], are typically dynamically allocated at the time the device or component joins a network. Within the RFID tag, either or both naming approaches may be used depending upon the complexity of the communication between components. A straightforward approach is to allocate a single unique identifier akin to a MAC to each tag functional component for tag micro-network communication and force the tag micronetwork gateway to maintain any mappings between the tag-micronetwork identifiers and any other identifiers that may be used for communication with off-tag components. The small number of components connected to a tag-micronetwork permits simple resource discovery to be used for on-tag components (e.g., a small table relating components and their communicating partners). The often immutable nature of tag functionality also permits static resource discovery to be performed at the time of tag manufacture.

4.2. Routing Strategies

The routing strategy determines how a message is sent through the network. If there is only a single physical path from one node to another node, then communication between these two nodes must follow that path. However, if multiple communication paths exist between two nodes, then one of those paths must be chosen for a specific message. The three most common routing strategies used in large networks are fixed routes, virtual circuits, and dynamic routes.

Within RFID reader-tag micronetworks, there exists only a single wireless path between readers and tags. When this wireless path between a reader and a tag is severed due to phenomena such as obstructions, distance, and noise, the reader is not able to communicate with, discover, or identify a tag.

Within an RFID tag micronetwork, there will exist a limited number of communication paths between two components. It is expected that most RFID tag micronetworks will afford exactly one communication path between two communicating components.

Therefore, micronetworks within RFID systems will most likely use fixed routes between devices and components.

4.3. Connection Strategies

Once two components or devices are able to communicate, the connection strategies determine how these components send a sequence of messages. The basic connection strategies are circuit switching, message switching, and packet switching.

In **circuit switching**, a permanent, dedicated physical link is established between the two communicating components or devices. This link is allocated for the duration of the communication and no other devices may utilize the communication channel until it is relinquished by the communicating parties.

In **message switching**, a temporary communication link is established between the communicating components or devices for the duration of the message. Multiple messages may utilize the same communication link.

In **packet switching**, a message is partitioned into a set of small, fixed-length messages referred to as **packets**, **frames**, or **datagrams**. Each packet is communicated over the communication network, and packets corresponding to parts of the same message may take different paths through the network. Packets must be reassembled at their destination.

Within an RFID reader-tag micronetwork, the wireless interface prevents the use of circuit switching and the low functionality on tags may prevent the use of packet switching. Consequently, message switching may be heavily used. In addition, the low communication bandwidth that a wireless communication channel affords requires the reader-tag messages to be as short as possible to achieve the desired communication.

Within an RFID tag micronetwork, the use of packet switching will be minimized. Packet switching requires components that have the capability to collect and reassemble packets to form a message. The RFID tag components are often lower functionality devices than is required for packet switching; therefore, circuit switching and message switching are more amenable to tag micronetworks.

4.4. Contention

Contention control determines how the network is shared and demand for the network is resolved. The common approaches in traditional networks are CSMA/CD, token passing, message slots, and centralized control.

Within an RFID reader-tag micronetwork, the reader controls the communication with all tags, and the identification anti-collision algorithm is used to control contention for the wireless channel by the tags. Reader anti-collision algorithms may be used for contention control between neighboring readers in the system [7][23][22].

Within an RFID tag micronetwork, a simple micronetwork controller may be used to control contention for the shared micronetworks. The micronetwork gateway may be used as the contention controller. More complex contention control approaches are not amenable to tag micronetworks due to the limited functionality of the connected components.

5. RFID MICRONETWORK COMMUNICATION PROTOCOL

An RFID system contains micronetworks embedded within micronetworks. Standard, packet-based communication protocols must be used over these micronetworks to enable exibility in the system functionality and capabilities. We review the IEEE 802.3 MAC packet used for local wired networks and the IEEE 802.11 MAC packet used for local wireless networks as examples of packet-based communication frames. We finish this section by presenting a MAC packet for RFID reader-tag communication and a PicoIP packet for on-tag micronetwork communication.

5.1. The Tag as a Mobile Network of Devices

A tag is a mobile embedded system with a micronetwork gateway and a micronetwork of functional units. As a mobile system, the fixed location and mobile readers must identify the tags, determine the functionality contained in each tag, and communicate with the tags to obtain data and information stored on them. In an environment containing ubiquitous RFID tags that may differ in their functionality, there must be a common set of functionality implemented by all devices. This core set of functionality is a resource discovery protocol and the ability to communicate using a basic communication protocol. Additional functionality implemented beyond the resource discovery protocol may vary from tag to tag; therefore, there is an absolute need to rely upon a standard communication protocol for accessing all on-device functionality beyond the resource discovery protocol. The communication protocol acts as a wrapper for the tag specific communication in a manner similar to how the 802.3 protocol acts as a wrapper for TCP/IP communication packets.

In RFID tags, the use of standardized communication interfaces to access on-tag functionality from a reader provides a common logical view of the communication micronetworks within the tag, regardless of their implementation and the functionality connected to them. The tag micronetwork gateway translates from the reader-tag communication protocol to the required micronetwork communication protocol implemented on that tag. This common interface enables a simplified reader-tag communication protocol that is exible enough to be usable for all on-tag micronetwork implementations and all possible on-tag functionality.

The reader-tag communication channel is a localized communication channel with the reader acting as a gateway to the tags. Occurring over a localized channel, the reader-tag communication protocol need

only operate over the lowest communication layers. These are the Data Link layer and the Physical layer in the OSI network model. The Data Link layer is responsible for the handling of communication packets, including any detection and recovery that occurred in the Physical layer. The Physical layer includes the actual signaling and encoding of symbols utilized in the communication. We do not consider the Physical layer in this paper; additionally, we do not consider higher level protocols that may be employed to ensure reliable communication.

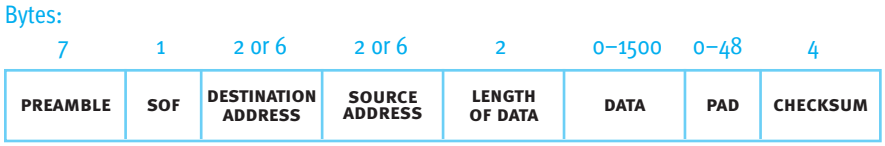
The Data Link layer communication protocols are referred to as Medium Access Control (MAC) protocols. MAC protocols include a standardized packet structure, a MAC packet (also referred to as a frame), for communication over the medium and a MAC protocol for controlling access to the medium. In the reader-tag communication channel, the MAC protocol is a solution to the Reader Collision Problem. We consider only the MAC packet here, as RFID MAC protocols have been addressed elsewhere [23][22].

5.2. Related Localized Communication Protocols

5.2.1. IEEE 802.3 Frame

Figure 1

IEEE 802.3 MAC PACKET (FRAME) FORMAT



The commonly used IEEE 802.3 MAC packet for wired networks is shown in Figure 1 [19]. Each frame begins with a Preamble of 7 bytes, each containing the bit pattern 1010 1010. The Preamble enables the receiving system's clock to synchronize with the sending system's clock.

The Start of Frame (SoF) byte, containing the bits 1010 1011, denotes the start of the frame itself.

The frame contains two addresses, one for the intended recipient of the the message, the **Destination Address**, and one for the sender of the message, the **Source Address**. The standard allows for either 2 byte or 6 byte addresses; however, the 10-Mbps and higher standards require the use of 6 byte addresses. The 6 byte addresses accommodate the 48-bit IEEE MAC addresses used to permanently and uniquely identify network interfaces.

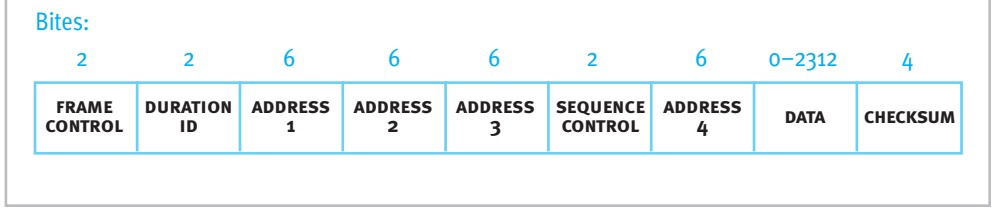
The **Length** field indicates the number of bytes present in the **Data** field, between 0 and 1500 bytes. The Data field has no constraints on it, and when the TCP/IP internetwork communication protocol is used, the Data field contains the TCP/IP communication packet. The 802.3 standard states that a frame must be at least 64 bytes in length to enable more efficient collision detection. The Pad field is used to fill out the frame to minimum size and may be between 0 and 48 bytes in length. The Pad value is zero for all Pad bytes.

The Checksum field is the final field in the 802.3 frame. The **Checksum** is a 32-bit cyclic redundancy check (CRC) used to detect errors in the transmission of the frame.

5.2.2. IEEE 802.11 Frame

Figure 2

IEEE 802.11 MAC PACKET (FRAME) FORMAT



The commonly used IEEE 802.11 MAC packet for wireless networks is shown in Figure 2 [18]. Unlike the IEEE 802.3 frame, the IEEE 802.11 frame does not contain a preamble for synchronization between sending system and receiving system. This synchronization is defined at the physical level since the 802.11 frame is designed to work across multiple frequency ranges, each with potentially significant differences in their synchronization requirements.

Each 802.11 frame begins with a **Frame Control** of 2 bytes. The Frame Control specifies the multiple global frame parameters that are to be used to interpret the frame contents.

The **Duration/ID**, consisting of two bytes, denotes either the length of time that this packet will require to be transmitted, including any handshaking required between sending system and receiving system, or the Station ID for the Power-Save poll message frame type.

The frame contains up to four addresses, **Address 1**, **Address 2**, **Address 3**, and **Address 4**. Their interpretation is dependent upon the To DS and From DS ags in the Frame Control. The addresses may be a Source Address, Destination Address, Transmitter Address, Receiver Address, or a Basic Service Set identifier (BSSID). All addresses are 6-bytes in length to accommodate the 48-bit IEEE MAC addresses used to permanently and uniquely identify each network interface. The Transmitter and Receiver addresses enable communication packets to be routed throughout the wireless network.

The **Sequence Control** field is used to identify where, within a sequence of communication frames, this frame belongs.

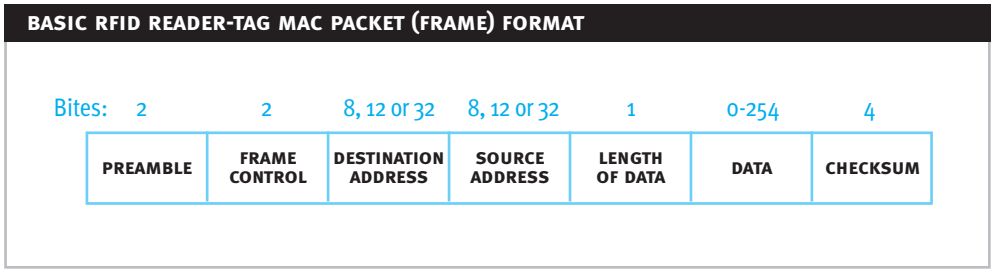
The **Data** field may have a length between 0 and 2312 bytes. The Data field has no constraints on the data it may contain, and when the TCP/IP internetwork communication protocol is used, the Data field contains the TCP/IP communication packet.

The **Checksum** field is the final field in the 802.11 frame. The Checksum is a 32-bit cyclic redundancy check (CRC) used to detect errors in the transmission of the frame.

5.3. RFID Frame for Reader-Tag Communication

The IEEE 802.3 and IEEE 802.11 frames illustrate the basic requirements for packetized communication on a localized network: synchronization, source address, destination address, and error detection. Additionally, the IEEE 802.11 frames illustrate the unique requirements of the wireless ad hoc networking environment and the need to be able to adapt to differing operating conditions. These considerations lead to a Basic RFID Reader-Tag frame format as shown in Figure 3.

Figure 3: Basic Frame



Each RFID frame begins with a **Preamble** of 2 bytes corresponding to the bit pattern 0000 0000 0000 0001. The Preamble enables the tag to synchronize with the reader's communication signal.

A two byte **Frame Control** follows the Preamble. The Frame Control specifies the multiple global frame parameters that are to be used to interpret the frame contents.

The frame contains two addresses, one for the intended recipient of the message, the **Destination Address**, and one for the sender of the message, the **Source Address**. A valid address in our context is an EPC™ which may be either 64-bits, 96-bits, or 256-bits in length.

The **Length** field indicates the number of bytes present in the **Data** field, between 0 and 254 bytes. The Data field has no constraints on its contents except that the length of the data must be an integer byte value.

The **Checksum** field is the final field in the RFID frame. The Checksum is a 32-bit cyclic redundancy check (CCITT CRC-32) used to detect errors in the transmission of the frame. There are six versions of the Checksum that may be used: authentication code (AC), secure authentication code (SAC), identity authentication code (IAC), secure identity authentication code (SIAC), broadcast authentication code (BAC), and secure broadcast authentication code (SBAC). The values over which each of these Checksums is calculated are given in Table I.

Table 1: Values over which the RFID Checksums are calculated.

CHECKSUM	CALCULATION VALUES
AC	Frame Control, Destination Address, Source Address, Length, Data
SAC	Frame Control, Destination Address, Source Address, Length, Data, Password
IAC	Frame Control, Destination Address, Length, Data
SIAC	Frame Control, Destination Address, Length, Data, Password
BAC	Frame Control, Length Data
SBAC	Frame Control, Length Data, Password

The narrow communication bandwidth available in the reader-tag communication channel encourages the communication of fewer bits if possible. We propose two additional frame variations to enable the communication of fewer bits over the reader-tag communication channel. The Private RFID Frame is shown in Figure 4. The Reduced RFID Frame is shown in Figure 5.

Figure 4: Private Frame

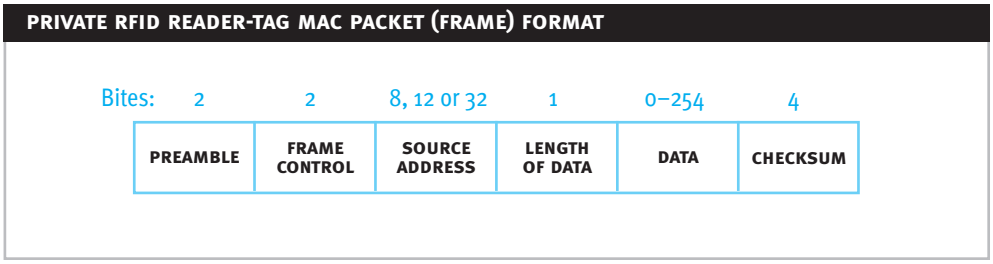
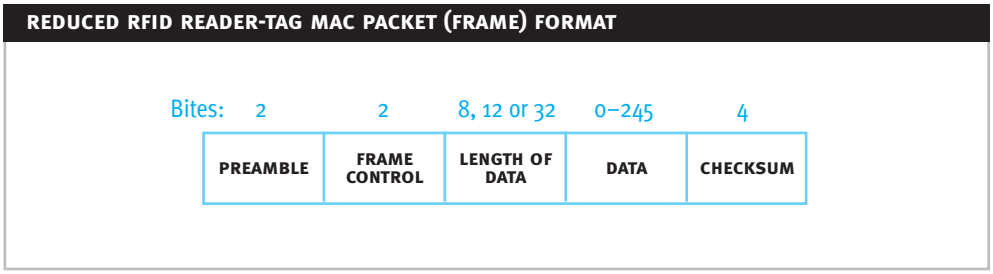


Figure 5: Reduced Frame



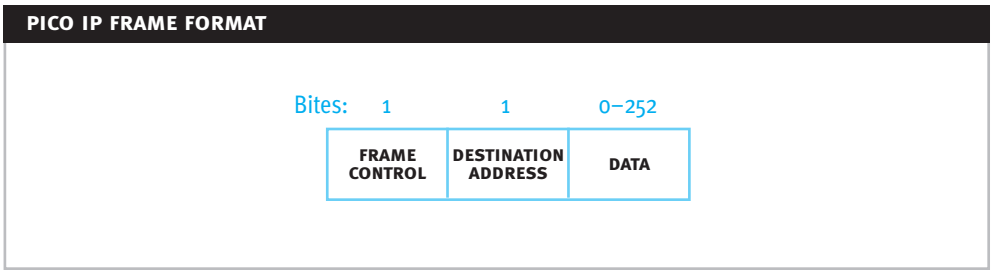
The Private RFID Frame reduces communication by not explicitly including the Destination Address within the frame. The Destination Address may be implicitly included in the frame by use of either the AC (SAC) or IAC (SIAC) Checksum (secure Checksum). In addition to reducing the number of bits communicated during a frame, the implicit inclusion of the Destination Address improves the privacy of the communication between readers and tags.

The Reduced RFID Frame reduces communication even further by explicitly including neither the Source Address nor the Destination Address. This has the added benefit of further improved privacy as well. The Destination Address may be implicitly included by use of either the AC (SAC) or the IAC (SIAC).

5.4. On-Tag Micronetwork Communication Frame

When the on-tag micronetwork gateway receives an RFID MAC Frame, it must determine the frame's validity and destination. If the frame is valid and intended for one of the functional components on the tag, the micronetwork gateway must analyze the Data in the RFID MAC Frame and forward the Data to the intended component to complete the communication. If no component is specified as the destination or the micronetwork gateway itself is the destination component, then the micronetwork gateway will evaluate the Data. If the Data is a command, the micronetwork gateway may execute the command and control the required components directly.

Figure 6: PicoIP Frame



Determining the destination component is simplified by formatting Data in the RFID MAC Frame in a standard format such as a PicoIP frame as shown in Figure 6. The PicoIP contains three field: **Frame Control, Destination Address,** and **Data**. The Frame Control specifies the multiple global frame parameters that are to be used to interpret the frame contents. The Destination Address is the on-tag address of the destination component. The Data is the data, information, or command being communicated to the component.

The micronetwork gateway may encapsulate the PicoIP within a micronetwork MAC Frame. However, the small size of the micronetwork and the limited functionality of the connected components limits the ability of the tag to utilize full MAC frames. Instead, the PicoIP frame can be utilized as a micro-MAC frame. Error detection may be implemented at the physical PHY level to detect the unlikely event that errors occur in the communication over the micronetwork.

6. CONCLUSIONS

We have presented a network-based approach to accessing on-tag functionality. In this approach, the reader communicates with the tag in a standardized RFID MAC Frame. The standardized portion of the frame acts as a wrapper to the commands that initiate tag-specific functionality and communicate with on-tag components. The tag's micronetwork gateways translates from the reader-tag communication packet to the on-tag micronetwork interface for the desired functionality. The generality of the reader-tag RFID MAC frame enables any on-tag functionality to be accessed by the reader and higher level communication functionality to be implemented on top of the MAC communication.

The use of a standard packetized communication between reader and tag enables the tag manufacturers to implement market demanded functionality without further involvement from the standards bodies. This enables timely implementation and sale of market demanded functionality while preserving the exibility and ubiquitousness of the RFID systems.

7. REFERENCES

1. **D. Brock, "The compact electronic product code — a 64-bit representation of the electronic product code".**
   Technical Report MIT-AUTOID-WH-008, Auto-ID Center, November 2001.

2. **D. Brock, "The electronic product code — a naming scheme for physical objects".**
   Technical Report MIT-AUTOID-WH-002, Auto-ID Center, January 2001.

3. **H. Chang, L. Cooke, M. Hunt, G. Martin, A. McNelly & L. Todd, "Surviving the SOC Revolution – A Guide to Platform-Based Design".**
   Kluwer Academic Publishers, 1999.

4. **W.J. Dally & B. Towles, "Route packets not wires: On-chip interconnection networks".**
   In Proceedings of the 38th Design Automation Conference, June 2001.

5. **D.W. Engels, "Epc-256: The 256-bit Electronic Product Code™ representation".**
   Technical Report MIT-AUTOID-TR-010, Auto-ID Center, February 2003.

6. **D.W. Engels, "The use of the electronic product code".**
   Technical Report MIT-AUTOID-TR-009, Auto-ID Center, February 2003.

7. **D.W. Engels & S.E. Sarma, "The reader collision problem".**
   In Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, October 2002.

8 **K. Finkenzeller, "RFID Handbook: Radio-Frequency Identification Fundamentals and Applications".**
   John Wiley & Sons Ltd, 1999.

9. **International Organization for Standardization (ISO) JTC 1/SC17.**
   ISO/IEC 15693:2000, Identification Cards, 2001.

10. **International Organization for Standardization (ISO) TC 104/SC 4.**
    ISO 10374:1991, Freight Containers – Automatic Identification, 2000.

11. **International Organization for Standardization (ISO)/IEC JTC 1/SC 31/WG 4/SG 3 N311.**
    ISO/IEC CD 18000-6, Information Technology — Radio Frequency Identification (RFID) for Item Management — Part 6: parameters for Air Interface Communications at 860-930 MHz, May 4, 2002.

12. **A. Hemani, A. Jantsch, S. Kumar, A. Postula, J. Oberg, M. Millberg & Dan Lindqvist, "Network on chip: An architecture for billion transistor era".**
    In Proceedings of the IEEE NorChip Conference, November 2000.

13. **R. Hinden & S. Deering, "IP Version 6 Addressing Architecture".**
    IETF, RFC 2373, July 1998. http://www.ietf.org/rfc/rfc2373.txt

14. **IBM, "CoreConnect Bus Architecture, 1999".**
    http://www.chips.ibm.com/products/coreconnect

15. **University of Southern California Information Sciences Institute, "Internet Protocol: DARPA Internet Program Protocol Specification".**
IETF, RFC 791, September 1981. http://www.ietf.org/rfc/rfc0791.txt

16. **K. Keutzer, S. Malik, R. Newton, J. Rabaey & A. Sangiovanni-Vincentelli, "System-level design: Orthogonalization of concerns and platform-based design."**
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 19(12):1523–1543, December 2000.

17. **ARM Limited, "AMBA Specification, Revision 2.0".**
May 1999. http://www.arm.com

18. **The Institute of Electronics and Inc. "(IEEE) Electronics Engineers".**
Ieee 802.11, 1999 edition (iso/iec 8802-11: 1999) ieee standards for information technology – telecommunications and information exchange between systems – local and metropolitan area network – specific requirements – part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, 1999.

19. **The Institute of Electronics and Inc, "(IEEE) Electronics Engineers".**
Ieee standards for local area networks: Carrier sense multiple access with collision detection (csma/cd) access method and physical layer specifications, New York, New York, 1985.

20. **D.C. Plummer, "An Ethernet Address Resolution Protocol".**
IETF, RFC 826, November 1982. http://www.ietf.org/rfc/rfc0826.txt.

21. **T. A. Scharfeld, "An analysis of the fundamental constraints on low cost passive radio-frequency identification system design".**
Master's thesis, Massachusetts Institute of Technology, 2001.

22. **J. Waldrop, D.W. Engels & S. E. Sarma, "Colorwave: A mac for RFID reader networks".**
In IEEE Wireless Communications and Networking Conference (WCNC03), March 2003.

23. **J. Waldrop, D.W. Engels & S.E. Sarma, "Colorwave: An anticollision algorithm for the reader collision problem".**
In IEEE International Conference on Communications (ICC03), May 2003.

24. **D. Wingard, "Micronetwork-based integration of socs".**
In Proceedings of the 38th Design Automation Conference, June 2001.

Designed by Foxner. www.foxner.com