The Pennsylvania State University

The Graduate School

Department of Electrical Engineering

RFID RADAR TAG SYSTEM DESIGN

USING ULTRAWIDEBAND NOISE WAVEFORMS

A Dissertation in

Electrical Engineering

by

Qihe Pan

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

December 2011

The dissertation of Qihe Pan was reviewed and approved* by the following:

Ram Narayanan
Professor of Electrical Engineering
Dissertation Advisor
Chair of Committee

Jim Breakall
Professor of Electrical Engineering

Douglas Werner
Professor of Electrical Engineering

Stephen Simpson
Professor of Mathematics

Kultegin Aydin
Professor of Electrical Engineering
Head of the Department of Electrical Engineering

*Signatures are on file in the Graduate School

ABSTRACT

Radio frequency identification (RFID) tags are small electronic devices working in the radio frequency range. They use wireless radio communications to automatically identify objects or people without the need for line-of-sight or contact, and are widely used in inventory tracking, object location, environmental monitoring due to their low cost, small size, and wireless functionality.

This dissertation explores the application of active RFID tags in outdoor environments responding to random noise radar interrogations with pre-determined messages. A conceptual system design for communication between radar and RFID tags using ultrawideband (UWB) noise waveforms is proposed and analyzed theoretically and via simulations. The tag structure comprises a sensing receiver and active receiver/transmitter. The sensing receiver senses the radar header consisting of a pre-arranged secret realization of the noise waveform. The active receiver/transmitter modulates the RFID tag's message onto the radar interrogation signal through weighted tapped delays and reradiates the tag message back to the radar. System performance is evaluated in terms of symbol error probability in an additive white Gaussian noise (AWGN) channel. An algorithm to combat multipath interferences on the RFID tag–to–radar link is presented. It is shown that this system is capable of communicating a suite of messages from the tags to the radar.

This dissertation also explores the application of active RFID tags in target discovery and information routing in the RFID networks. The design of a covert RFID tag network for target discovery and target information routing is presented. In the design, a static or very slowly moving target in the field of RFID tags transmits a distinct pseudo-noise signal, and the RFID tags in the network collect the target information and route it to the command center. A map of each RFID tag's location is saved at command center, which can determine where a RFID tag is

located based on each RFID tag's ID. The target information collection method with target association and clustering, and the information routing algorithm within the RFID tag network are proposed. The design and operation of the proposed algorithms are illustrated through examples. Simulation results demonstrate the effectiveness of the design.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my research advisor, Dr. Ram Narayanan, for his guidance, support, and for his patience and encouragement during my study at Penn State. I am also very grateful to Dr. Jim Breakall, Dr. Douglas Werner, and Dr. Stephen Simpson. I acknowledge their service and guidance as my committee members, and for their insightful suggestions and comments on my work. I would also like to thank all professors who have imparted to knowledge in my study.

I also acknowledge funding support from the Air Force Office of Scientific Research (AFOSR) Grant # FA9550-06-1-0029, and for Dr. Jon Sjogren of AFOSR for his encouragement and comments.

My deepest appreciation goes to my parents. I sincerely thank them for their consistent love, support, and encouragement all through the years.

Chapter 1

Introduction

1.1 Background

1.1.1 RFID tags

Radio frequency (RF) tags, also known as radio frequency identification (RFID) tags, are small electronic devices typically adhering to objects of interest which can communicate with a tag interrogator through a wireless channel. They have the advantage of being read through a variety of visually and environmentally challenging conditions, such as building walls and foliage, where barcodes or other optically read technologies will not work [1], [2]. Their properties such as low cost, small size, and wireless functioning make them widely used in inventory tracking [3], object location [4], environmental monitoring [5], environmental management [6], personnel identification [7], etc. RFID tags are also good candidate technologies for combat identification (CID), which provide the necessary awareness to identify friendly combat entities and avoid fratricide [8]. An RFID tag can also operate as a data carrier, where information can be written to the tag. Radar-responsive tags have both military applications, such as battlefield situational awareness, combat identification, targeting, personnel recovery, and unattended ground sensing, as well as government applications, such as nonproliferation, counter-drug, search-and-rescue, and land mapping [9]. There are three types of RFID tags based on the characteristics of the power source: passive, semi-passive, and active. Passive tags use the energy from the incoming signal to power themselves and they have practical read distances from about

10 cm up to a few meters. Semi-passive and active tags require an internal power source, usually a small battery, and thus have longer operating distances up to hundreds of meters [10].

Using the reflected power for communications, dating back to the late 1940s, was an insightful exploitation of radar systems for multifunctional usage [11]. In [12], an electronic identification system which uses modulated backscatter from an RF beam-powered tag is described, where the reader transmits a single frequency RF signal, and a subcarrier is used in the return signal format for achieving clutter suppression. A controllable radar reflector consisting of an array of resonant dipoles or slots combined with a reflecting plate was used to establish passive telemetry system for transferring information from the site of a target to a radar station [13]. Backscatter modulation is a suitable modulation scheme for tagging because no RF source is needed for the remote devices. Such a tagging system has been proposed wherein frequency hopping combined with backscatter modulation is used for interrogating the tag [14].

A programmable covert radio tag able to communicate with a variety of RF pseudo-random modulated waveforms emitted from a source of interrogating energy was developed so that military troops wearing the RF tag could operate undetected [15]. A scheme to embed the communication signal within the radar backscatter using a tag/transponder on an intra-pulse basis is proposed in [16]. Their approach is based upon eigen-decomposition of the collection of delay shifts of the incident radar waveform. Another scheme to ensure covertness is through the use of noisy tags, which are regular RFID tags that generate noise. These have been used to establish secret keys on-the-fly between the reader and the tag, so that an eavesdropper would only hear the noise, but the intelligent receiver could subtract the noise and recover the intended signal [17]. A technique to identify multiple tags simultaneously by weighting and combining the in-phase (I) and quadrature (Q) channel signals was implemented in [18]. The concept of orthogonal frequency coding (OFC) offers enhanced processing gain, lower interrogation power spectral density (PSD), and the possibility of adding pseudo-noise coding for covertness [19].

1.1.2 Noise radar

A general mathematical formulation of the intra-pulse radar-embedded communication in the ambient radar scatter interference is provided in [20]. Linear frequency modulated (LFM) waveforms are also candidates for radar communications, which uses signal processing rather than hardware to mitigate the interference problem [21]. Chirp waveforms are used in [22], wherein a multifunctional UWB communication and radar system has been designed and implemented. Other aspects of relevance to the radar communication system, such as the candidate radar types, sharing of resources, etc. are discussed in [23]. As part of the Department of Defense Future Combat System (FCS) philosophy, each element of a network-centric force, e.g., a radar sensor and an unmanned aerial vehicle (UAV), is expected to possess an embedded communications capability [24].

While narrow band noise radars have been proposed and refined over the past fifty years [25]–[31], the concept of UWB random noise radar has seen significant development more recently [32]–[37]. In contrast to conventional radar, the UWB noise radar transmits a noise or noise-like waveform having a fractional bandwidth of greater than 25%. The return from the target is cross-correlated with a time-delayed replica of the transmit waveform to determine the range to the target with a range resolution inversely proportional to the bandwidth. A simplified noise radar architecture is shown in Figure 1.1. The noise source sends a noise or noise-like signal to the power splitter. One branch of the power splitter output goes to the amplifier and is transmitted through the antenna. The other branch of the power splitter output goes to the correlation receiver, where it's cross correlated with the amplified received signal to determine the range to the target.

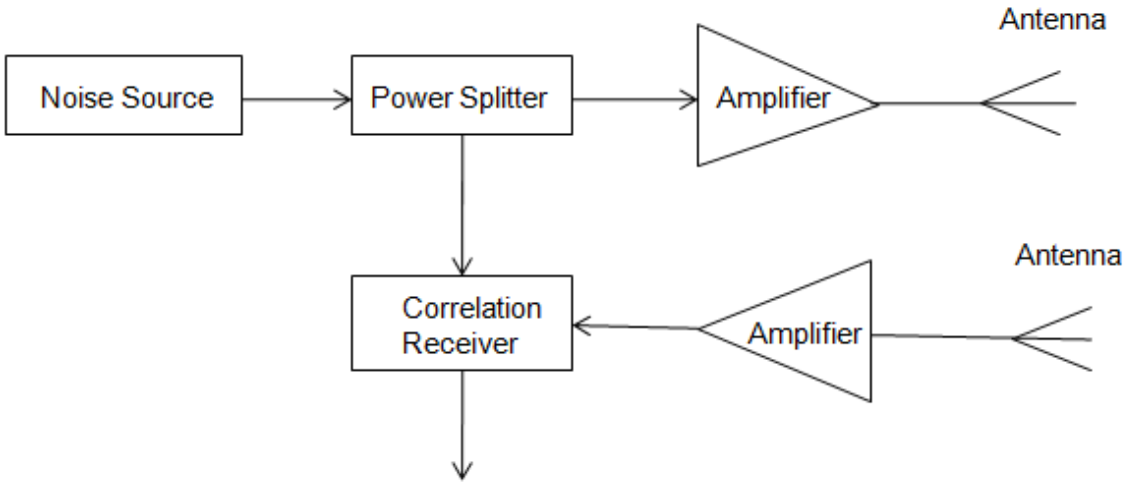


Figure 1.1. A simplified noise radar architecture.

Noise radars satisfy important requirements for military systems, such as low probability of interception (LPI) and low probability of detection (LPD), owing to the featureless characteristics of its waveform [38]. Moreover, the aperiodicity of the waveform also causes the suppressed ambiguity in range/velocity [39]. Another advantage of UWB noise radars is their ability to efficiently share the frequency spectrum. A number of UWB noise radars can operate over the same frequency band with minimal cross-interference since each noise waveform is uncorrelated with the others.

1.2 Motivation

RFID technology and its application have attracted a lot of attention in recent years, and become a hot research area. In [40], a literature review on RFID research that was published between 1995 and 2005 is presented. The RFID literature in the review was classified into four major categories: RFID technology, RFID applications, policy and security issues, and others. Article on RFID technology pertain directly to the RFID system, which was divided into the

following subcategories: tags and antennas, reader, and communication infrastructure. Privacy issues on RFID mainly relate to potential misuse of data by unauthorized users leading to illegal use of personal information. Securities concerns involve vulnerabilities and the protection of confidential data from unauthorized access and manipulation. One of the security problems is the illicit tracking of RFID tags. Other security problems are confidentiality, integrity, authentication, authorization, non-repudiation, and anonymity. Most of the articles on other topics are general introductions or reviews of RFID technology, and some are related to the general usage of RFID.

According to the review in [40], a majority of the articles are related to RFID technology, while the fewest being published are on policy and security issues. Recent research on RFID tag systems mainly focuses on tags and antennas. The specific area of research includes tag design and testing, performance analysis, manufacturing process, materials and process development, power sources for passive tags, antenna design and placement. It is agreed that the cost and performance of the tag are very important in determining the cost and performance of the whole system. However, there are relatively few articles on the associated communication infrastructure. As for the application of RFID technology, library services and retailing are the applications with the most publications.

There are many challenges to be overcome before the extensive applications of RFID are realized. Areas of RFID research that merit future attention include strategic and operational design considerations, such as system design and number of antennas to be installed, privacy and security issues, etc.

While most of the RFID research concentrates on RFID technology and in particular its components, there is a need to provide useful guiding principles for the process of RFID system design, development, implementation, and evaluation, as pointed out in [40]. Future research effort is needed in this area. Studies that involve the design, implementation, and deployment of RFID technology should be an emphasis in the future research direction.

In this research, the application of active RFID tags in outdoor environments responding to random noise radar interrogations with pre-determined messages is explored, and the application of RFID tags in target discovery and target's information routing in the RFID tag network using a pseudo-noise signal is also explored. A conceptual system design for communication between radar and RFID tags using ultrawideband (UWB) noise waveforms is proposed and analyzed theoretically and via simulations. The design of a covert RFID tag network for target discovery and target information routing is presented.

The first RFID tag application scenario in the research is depicted in Figure 1.2. In this application, radar sends out interrogation signals to gather the assets' conditions, and RFID tags associated with assets in the field respond to the radar with appropriate messages. The proposed RFID tag is able to send various kinds of messages from its associated asset.

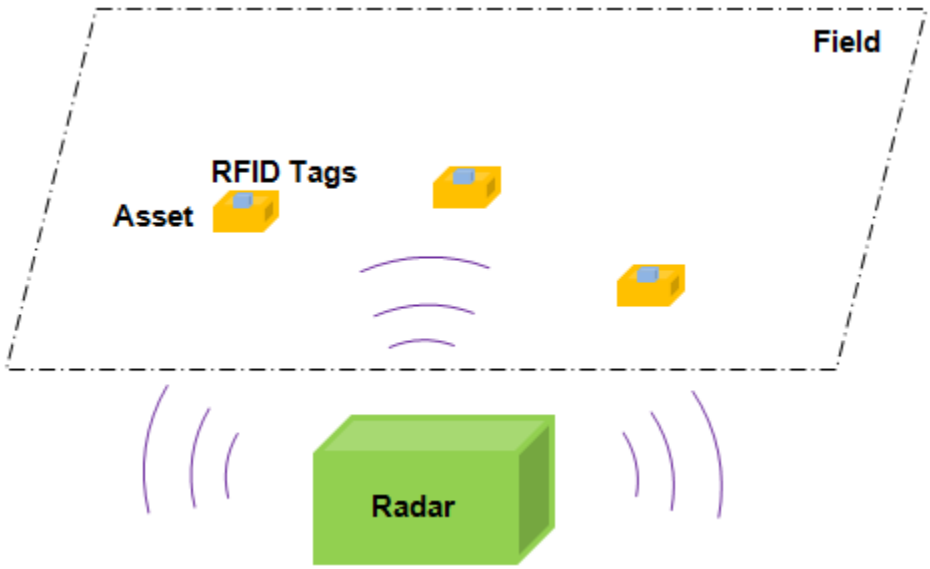


Figure 1.2. RFID tag application scenario I.

The goal of this part of the research is to design an RFID tag system which helps radar recognize and collect information of friendly assets in the outdoor in a covert manner.

The second RFID application scenario in the research is depicted in Figure 1.3. A static or slowly moving target is in the field of RFID tags, out of the range of the command center. The cooperative target transmits a distinct RF pseudo-noise signal. The goal of the RFID tag network design is to collect the target's information and route it to the command center with assistance of the deployed RFID tags. The RFID tags here do not know their own locations. A map of their locations is saved at the command center, so the command center can determine where a RFID tag is located based on the RFID tag's ID.

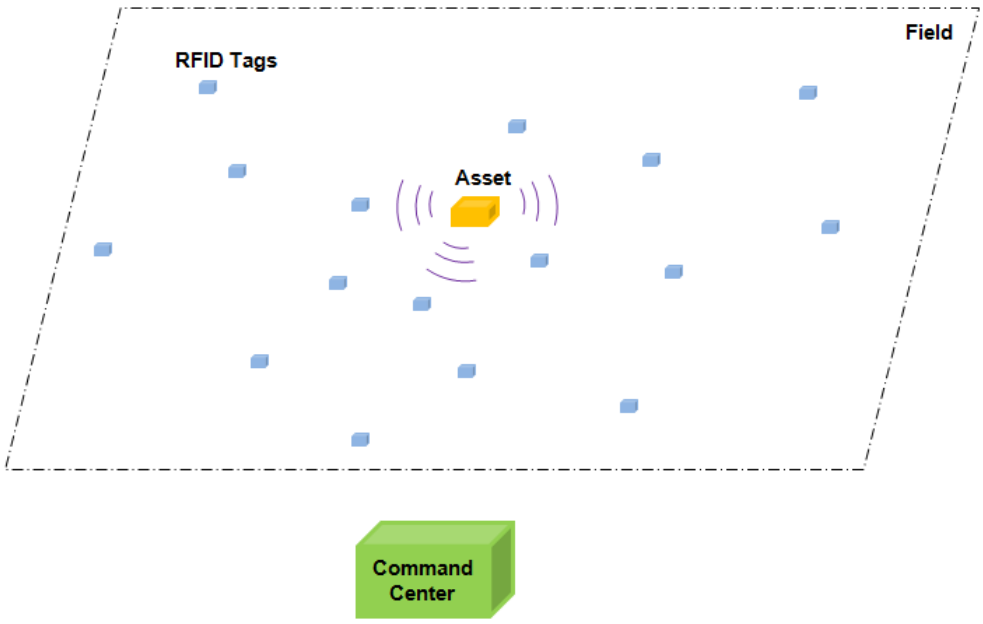


Figure 1.3. RFID tag application scenario II.

In this dissertation, a conceptual design of an RFID tag responding system for application I is proposed to assist a noise radar in collecting relevant information on slowly-moving assets and tracking their whereabouts in an outdoor environment, inspired by the results of recent research [41], [42]. In the proposed design of the system, the RFID tag functional block comprises two parts: the sensing receiver and the active receiver/transmitter considering the

efficiency of energy consumption. The sensing receiver senses the radar header consisting of a pre-arranged secret realization of the noise waveform. The active receiver/transmitter modulates the RFID tag's message onto the radar interrogation signal through weighted tapped delays and reradiates the tag message back to the radar. The RFID tag's ID is embedded through the frequency band of its transmitted signal. In our approach, a UWB noise waveform is chosen as the probing signal owing to its low probability of detection and interception capabilities as well as its immunity from interference and jamming. The waveform is generated by amplifying and bandpass filtering the thermal noise generated by a resistor; thus, the waveform is not to be considered to be pseudo-noise, the latter being generated deterministically and therefore possessing a cyclic autocorrelation function. Since the UWB noise signal used as the information carrier is easy to generate, it simplifies the system implementation while achieving a fair amount of covertness. It may certainly be possible to detect a true thermally-generated noise signal embedded in ambient noise, but only if adequate time and processing resources are available, which is unlikely in the scenarios considered. The operation of the system is demonstrated and the performance of the system is evaluated in terms of symbol error probability in an additive white Gaussian noise (AWGN) channel. An algorithm to combat the multipath interferences on the RFID tag–to–radar link for the proposed system is presented.

It is shown that this system is capable of communicating a suite of messages from the tags to the radar. The maximum number of messages the tag is capable of conveying is determined by the length of its delay line. Furthermore, the proposed RFID tag responding system is able to operate covertly in the sense that its symbol error rate (SER) is still small under very low channel signal-to-noise ratio (SNR).

An RFID tag network for target discovery and target's information routing for application II is designed in this dissertation. In the design, a static or slowly moving target in the field of RFID tags transmits a distinct pseudo-noise signal, and the RFID tags in the network collect the

target information and route it to the command center. The noise signal from the target is known only to the RFID tags in the network so they can easily detect it. However, this signal is not detected by undesired parties since the transmitted signal has unpredictable random-like behavior and does not possess repeatable features for signal identification purposes [38]. A map of each RFID tag's location is saved at command center, which can determine where a RFID tag is located based on each RFID tag's ID.

In the design, RFID tag clusters within the RFID tag network are employed to collect the target's information. There are two steps in this process: (1) target association, and (2) cluster formation and cluster head selection. If an RFID tag detects the target, then it stores the target's ID and gets associated with the target. Clusters are formed by RFID tags associated with the same target. One of these RFID tags, selected as the head of the RFID tag cluster, routes the target's information out to the command center. In our design, the RFID tag with the maximum number of links to the outside of the cluster is selected as cluster head, which is robust to channel failures, considering that the RFID tags in the network are battery driven and may run out of life. When some of the communication links between the cluster head and those RFID tags out of the cluster are broken, the cluster head RFID tag still can use alternate communication links between it and RFID tags outside of the cluster to route the target's information out.

In our proposed information routing algorithm within the RFID tag network, the routing path in the RFID tag network from cluster head RFID tag to the command center is selected according to the channel condition, which is a joint optimization of favorable channel conditions and short path length. Each RFID tag intelligently selects its successor and routes the target's information to it. There are two stages when each node selects its successor on the routing path based on two criteria: (1) channel quality sensing, and (2) target's information routing. During channel quality sensing, the channel condition is estimated and quantized to form the link weight,

while in the information routing stage, the RFID tag determines its successor based on the channel information obtained and sends the target's information to it.

The design and operations of the proposed algorithms are illustrated through examples. Simulation results clearly demonstrate the effectiveness of the design.

1.3 Organization of the dissertation

This dissertation is organized as follows. An RFID Tag — Radar system model is presented in Chapter 2. The system operation is illustrated and the system performance is analyzed in Chapter 3. A technique to combat multipath interferences for the proposed system is also presented in Chapter 3. Chapter 3 also discusses the implementation considerations of the system. Design of a covert RFID tag network for target discovery and target's information routing is presented in Chapter 4, where target information collecting and routing algorithms are discussed, and illustrated through examples. Finally Chapter 5 draws the conclusions of the dissertation, and points out future work.

Chapter 2

RFID tag — Radar system model

2.1 Introduction and motivation

RFID (radio frequency identification) uses radio communication to identify objects. An RFID system typically insists of three components: RFID tags, readers and a host computer. RFID tags are small electronic devices usually attached to objects of interest which can communicate with a tag interrogator through a wireless channel. An RFID tag consists of a microchip and an antenna. Each RFID tag is uniquely identified by a tag ID stored in its memory. RFID reader, or interrogator, requests or alters information contained in an RFID tag by sending RF signals to it. If an RFID tag is in the range of the reader, it will respond with its ID and data. The reader then decodes its received signal and sends data to the host computer for further processing [43].

RFID is drawing increased attention recently due to its benefits and its dropping cost. It provides benefits such as that it does not require line-of sight to operate and that it can be read through a lot of visually and environmentally challenging conditions mentioned in Chapter 1. Though RFID is increasingly used, most of its current applications are very simple and mainly focus on item tracking and collecting data without intelligence [43]. Also, an RFID tag usually does not equip with high power security mechanism due to the limitation of space and cost of it, therefore it is amenable to attack [43].

In our research, we explored the applications of active RFID tags in outdoor environments responding to random noise radar interrogations with pre-determined messages, and proposed a conceptual design of an RFID tag responding system to assist a noise radar in -

collecting relevant information on slowly-moving assets in an outdoor environment. RFID tags in the proposed system are able to sends back various kinds of messages which indicate different conditions of the targets they are attached to upon the radar's interrogation. This RFID responding system is designed to operate in a covert manner, where the data are well protected from detection and analysis from undesired parties. Symbol error probability of the system is still low in a very noisy channel.

In this chapter, a conceptual system design for communication between radar and RF tags using ultrawideband (UWB) noise waveforms is presented and analyzed theoretically and via simulations. In the scenario, the radar sends out interrogation signals of noise waveform to gather the assets' conditions, and RFID tags associated with assets in the field respond to the radar with appropriate messages. Active RFID tags are applied in the system due to their performance advantages. Active RFID tags do not employ backscatter mechanism for communication to the reader. Instead, they use batteries to power their digital logics and transmissions. Thus, they are less susceptible to environmental factors and poor electromagnetic propagation. The increased sophistication of the active RFID tag also provides for greatly increased reading range, increased security, increased resistance to interference, and increased functionality [44]. The maximum number of messages an RFID tag in the system is capable of conveying is determined by the length of its delay line. The proposed RFID tag responding system is able to operate covertly in the sense that its symbol error rate (SER) is still small under very low channel signal-to-noise ratio (SNR). In our approach, a UWB noise waveform is chosen as the probing signal owing to its low probability of detection and interception capabilities as well as its immunity from interference and jamming. The waveform is generated by amplifying and bandpass filtering the thermal noise generated by a resistor; thus, the waveform is not to be considered to be pseudo-noise, the latter being generated deterministically and therefore possessing a cyclic autocorrelation function. Since the UWB noise signal used as the information carrier is easy to

generate, it simplifies the system implementation while achieving a fair amount of covertness. It may certainly be possible to detect a true thermally-generated noise signal embedded in ambient noise, but only if adequate time and processing resources are available, which is unlikely in the scenarios considered in this chapter.

This chapter is organized as follows. In Section 2.2, previous work on RFID systems are reviewed. In Section 2.3, the system model is described, where the design of radar transmitted signal, RFID tag architecture, and radar detector architecture is illustrated.

2.2 Previous work on RFID systems

As mentioned in Chapter 1, recent research on RFID tag systems mainly focuses on tags and antennas, while there are relative few articles on the associated communication infrastructure. Most of previous RFID systems are designed for identification and localization, with applications in libraries and the supply chain. More intelligent RFID systems, which have more information storage and processing capabilities, can be designed to have advanced functionalities, such as communicating with various messages about the object. Power efficiency is an issue to be taken into account in the RFID system design. RFID tag structure should be designed as simple and less energy consuming while achieving good system performance. Besides, a lot of current RFID systems are lack of privacy and security, and subject to external interferences threat. More secure RFID systems or covert RFID systems may be explored.

2.2.1 RFID systems with simple responses

A 3-D RFID system with a union tag is proposed for objects recognition in [45]. In this system, an object with a 3-D tag can be identified, and its location and orientation can be

estimated by analyzing the characteristics of the 3-D tag. However, complete recognition may not be possible. The 3-D tag is designed in regular hexahedron shape, which includes an RFID transponder and six tag antennas. Each tag antenna has unidirectional radiation pattern, and provides its own directional information to the transponder when it detects the power from the reader. Then the transponder transmits the identification signal with orientation to the reader. The 3-D tag, referred to as the union tag is implemented using six passive tags attached to six edges of a cube in [45]. The surface of the cube has shielding with metallic covering to block out the symmetric wave from undesirable direction. The passive tags have λ/2 dipole antennas, called the tag units, and each tag transmits its directional information to the reader. In union tag's location estimation, when two RFID reader antennas' locations are set, the two main lobe directions can be visualized by exploiting the characteristics of the unidirectional radiation pattern of the RFID antenna. Then the location of the tagged object can be estimated via trigonometry. Orientation of the object with the built-in union tag is classified into twenty-four poses depending on the direction of the view, and is determined by detecting two neighboring tag units.

An RFID tag system to sense the target's permittivity based on variations of backscattered power detected by the reader is presented in [46]. A multi-port passive tag with multiple chips concept is proposed, which is that when the target geometry is fixed and several reference permittivities are chosen, the impedance at the *n*-th port of the tag is matched to the chip if the tagged object's permittivity is ε_n. The ports of the tag will be differently mismatched, and will backscatter signals independently, carrying information of the target's permittivity. Backscattered power ratio between the received powers by the reader is calculated, and then the value of the target's permittivity is estimated using a pre-determined calibration curve showing the target's permittivity as a function of the backscattered power ratio. Although this system is able to estimate the target's permittivity without *a priori* knowledge of the target's position and orientation with respect to the reader, it requires preliminary electromagnetic processing to

produce calibration curves for the specific class of targets, and the obtained database and target's permittivity retrieval procedure need to be embedded in the reader [46].

2.2.2 RFID system protocols

In passive RFID systems, RFID tags use the energy from the reader interrogation signal to power themselves, and send back to the reader their IDs or information about the objects they are attached to. In the RFID tag reading process, if there are multiple tags responding to the reader at the same time, the signals from the tags will collide in time since the RFID tags communicate over a shared wireless channel. Thus the reader may not correctly recognize all the RFID tags. Besides, passive RFID tags are low functional and may not be able to communicate with each other to figure out the order to speak. Many RFID tag anti-collision protocols are studied in previous research. Some of the most common ones are Slotted Aloha, Adaptive Binary Tree, and the EPC Gen2 specification [47].

Slotted Aloha [47]

In this protocol, the reader first sends out a REQUEST command, which provides the available slots for the tags to use. Each tag randomly selects one of the slots, and broadcasts its ID at its chosen slot. Upon receiving a clear tag ID with no collisions in a particular time slot, the reader sends out a SELECT command containing that ID. Only the tag with that ID responds to the reader. Then the reader sends out a READ command, and that tag sends its corresponding information to the reader. Afterwards, the reader starts next conversation with the tags by sending out another REQUEST command.

This protocol can reduce tag collisions. With fewer slots provided by the reader, the reading process is faster. But when lots of tags are present in the reader's range, more slots are needed for fewer collisions. It may occur that one particular tag needs to wait for a long time to be read.

Adaptive Binary Tree [47]

This protocol uses a binary search to find one tag among many tags. The singulation is based on the tag's EPC ID or its pseudo ID. The basic idea of the tree traversal procedure is as follows. When a tag is involved in this procedure, it immediately sends out the most significant bit of its ID. The reader responds with a bit. If it matches the bit the tags sent, the tag will send the next bit of its ID. Otherwise, the tag will not respond, and it will wait for a data null from the reader to proceed to the tree traversal. At the boundary bit of the tag's ID, after the tag sends out the bit, if the reader confirms it, the tag sends the same bit again. Then if the reader responds with a 1 or 0, the tag will not respond, and it will wait for a data null from the reader to proceed to the tree traversal. If the reader responds with a data null, the tag will enter the Singulated Command Start state. In this state, if the tag receives a 0, it will go to the initial state and be indicated that it has been read. If the tag receives a 1, it will go to the Singulated Command state, where it receives 8-bit commands from the reader.

EPC Gen2 [47]

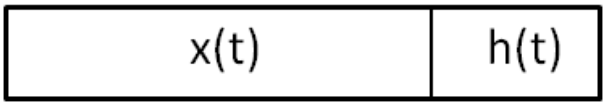
This protocol supports faster tag singulation. It considers the situation where two readers are in the same operating environment, within one kilometer of each other.

For communication between readers and tags, there are three procedures in this protocol. A reader may SELECT tags by asking tags to compare themselves to a bitmask. It may INVENTORY tags by singulating tags until it has recognized each tag within the range. It may also ACCESS tags, which includes reading information from a tag, writing information to a tag, killing a tag, etc.

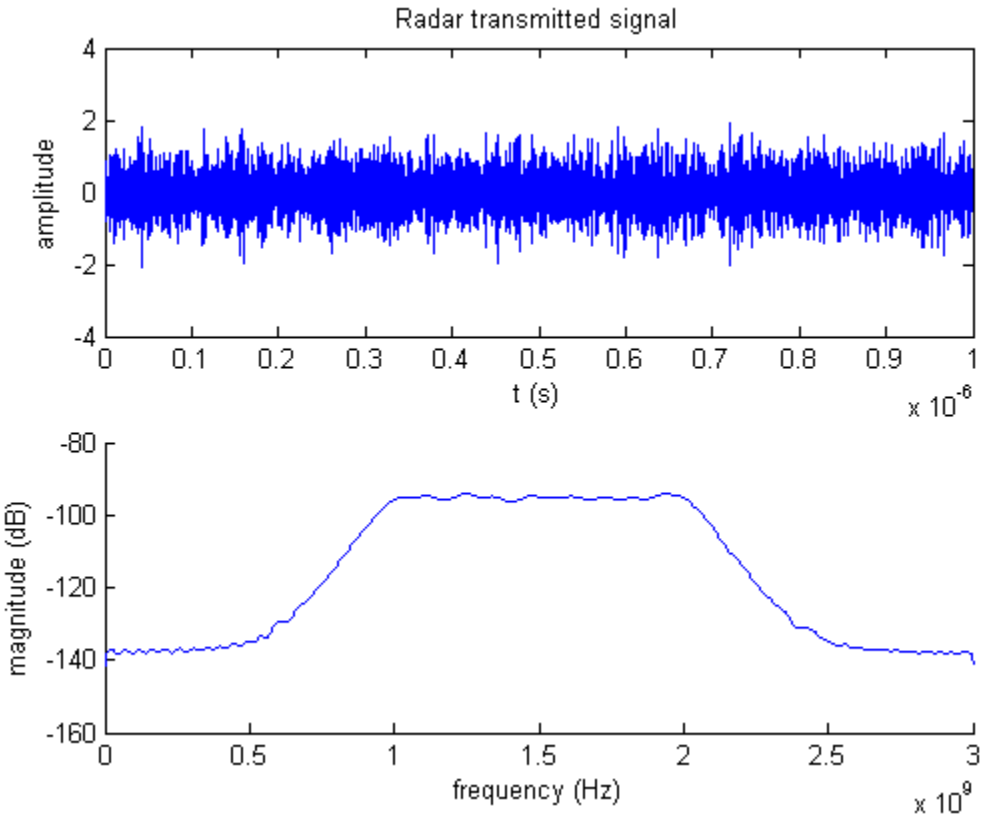
2.3 System model

2.3.1 Radar transmitted signal

Radar transmitted UWB noise signal has the form as shown in Figure 2.1, which is composed of two parts $h(t)$ and $x(t)$. The first part of the signal $h(t)$ is the radar header appearing in time before the radar interrogation signal $x(t)$. The radar header signal occupies a small fraction of the entire radar transmit signal. The interrogation signal $x(t)$ is a bandlimited UWB white Gaussian noise (WGN) radar waveform operating over the frequency range $[\omega_L, \omega_H]$. The header signal $h(t)$ is a prearranged and secret noise waveform realization also known by the RFID tag, and it exists over the same frequency band as $x(t)$. The radar header $h(t)$ is used to trigger the RFID tag. Once the RFID tag detects the radar header, it starts to modulate its message onto the radar interrogation signal $x(t)$. Since $h(t)$ is a noise signal only known to the radar and the RFID tag, the adversary cannot detect or forge it easily. This guarantees that the communication between the radar and the tag is covert and also that the RFID tag cannot be triggered by the adversary intentionally.



(a)



(b)

Figure 2.4. Radar transmitted signal: (a) signal format, and (b) time (top) and frequency (bottom) domain representations.

The header of radar transmitted signal can be randomly selected from a suite of pre-assigned random headers to better protect it from detection by undesired parties. However, this increases the complexity of RFID tag's architecture and RFID tag's energy consumption during the detection of radar header. This is because the RFID tag in the system needs to store the entire suite of radar headers beforehand and correlate its received signal with each stored radar header

to determine whether the incoming signal is from the radar. Furthermore, the RFID tag in our system is battery powered for longer range and advanced functionalities, and its energy consumption is also of concern in the system design. Instead, we propose that the radar header remains the same random waveform for each radar interrogation. Since this single radar header signal used in our system has randomness features, it is relatively difficult to be detected.

2.3.2 RFID tag architecture

The RFID tag functional block diagram is shown in Figure 2.2. It consists of two parts: a sensing receiver, and an active receiver/transmitter. The sensing receiver is merely a listening device which uses moderate amounts of power and is used to sense the radar header. The active receiver/transmitter is turned on once it gets an indication signal from the sensing receiver output that the radar header is detected. Upon receiving this wake-up call, it begins to receive and process the rest of the incoming signal, embeds the appropriate RFID tag message, and retransmits the message bearing RFID tag signal back to the radar.

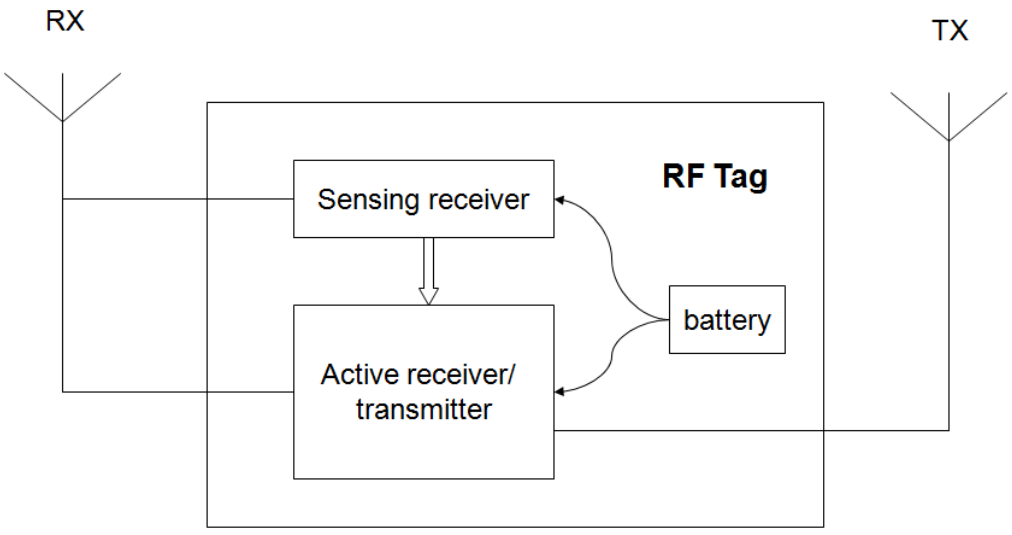


Figure 2.5. RFID tag functional block diagram.

The RFID tag operates in two modes: working mode and sleep mode. In the working mode, once the sensing receiver detects the radar header and sends a control signal to the active receiver/transmitter to turn on, the sensing receiver turns off. The active receiver/transmitter also turns off after completing the delay-modulating of the radar inquiry signal. Thus the entire RFID tag goes into the sleep mode after it is triggered. It will stay in the sleep mode for a period which is longer than the maximum multipath delay. Then the sensing receiver turns on again, waiting for the next radar header to arrive. Now the entire RFID tag is in the working mode again. This way, the RFID tag will not be triggered by the multipath signals in the radar to tag link, and it will not miss the radar's inquiry. Besides, the RFID tag is not always in working mode, and thereby improving its energy efficiency.

The sensing receiver functional block diagram is depicted in Figure 2.3. The bandpass filtered received signal is cross correlated with a replica of the radar header, which is saved at the RFID tag *a priori*. The output of the correlator goes through a threshold detector whose output controls the RFID tag's active receiver/transmitter. If the output of the correlator exceeds the threshold at some observing time, then the active transmitter/receiver is turned on.

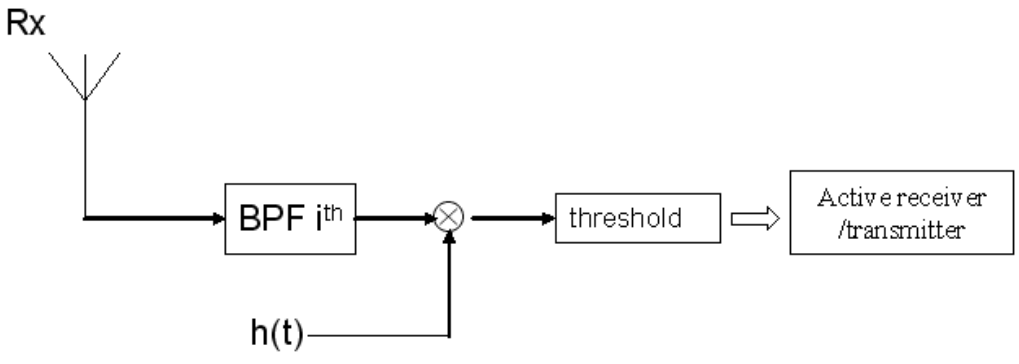


Figure 2.6. RFID tag sensing receiver block diagram.

The RFID tag active receiver/transmitter functional block diagram is shown in Figure 2.4. If and only if the radar wake-up signal is detected by the RFID tag sensing receiver, then the RFID tag active receiver/transmitter is enabled. The remaining portion of the radar signal, namely, the radar information bearing signal $x(t)$, is intercepted at the RFID tag. First this signal goes through a bandpass filter with bandwidth $\Delta\omega$ and center frequency ω_i, which covers part of the entire bandwidth of radar signal $x(t)$. This frequency index i represents the index of the i-th RFID tag. We assume that there is a fixed number of RFID tags within the radar's range during one interrogation duration. Since the delayed transmitted signal by the RFID tag does not contain the radar header, its sensing receiver will disregard it without further processing. Thus, loops causing chaotic or oscillatory behavior will be avoided in the tag's active receiver/transmitter circuit.

The entire bandwidth of the radar signal is divided into several subbands without mutual overlap by the RFID tags, all of the same bandwidth $\Delta\omega$, with center frequencies ranging from ω_1 to ω_N, where N is the total number of RFID tags, as shown in Figure 2.5.

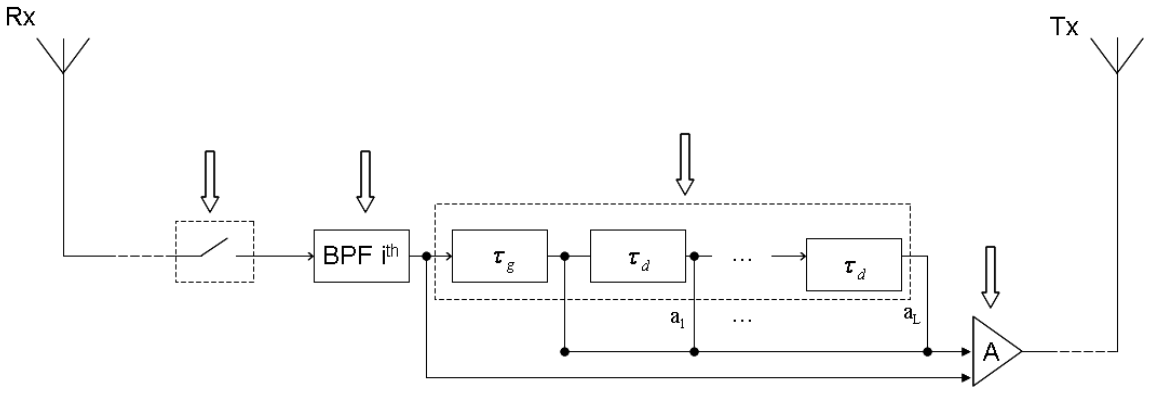


Figure 2.7. RFID tag active receiver/transmitter architecture.

Figure 2.8. Frequency band allocation for RFID tags.

A guard band between adjacent bands of the RFID tags is maintained in order to avoid interference between individual tags and to allow for the Doppler shifts associated with moving tags. The output of the bandpass filter at each RFID tag can be shown to be uncorrelated with each other. The Doppler frequency shift of the RFID tag is calculated as $f_d = 2v_r/\lambda = 2f_0 v_r/c$, where v_r is the radial velocity and f_0 is the radar frequency. For an RFID tag moving at the speed of 20 km/h and a radar operating over a frequency band of 1−2 GHz, the maximum Doppler shift is computed as 74 Hz. Since the RFID tag is considered mainly for associating with slowly-moving assets, as long as the guard band is designed to be large enough compared to the maximum expected Doppler shift, the effects of the Doppler shift can be neglected and there will arise no confusion for the detection of different RFID tags.

If the number of RFID tags in the radar's range is not fixed, the radar interrogation signal's frequency band can be divided into $N_{\max}$ subbands, where $N_{\max}$ is the maximum number of RFID tags attached to objects in the system. Each RFID tag occupies its distinct subband.

Next, one branch of the bandpass filter output $x_i(t)$ is passed through a weighted tapped delay line to embed the RFID tag's message. It is first delayed by the time τ_g, which is specifically designed such that it is longer than the radar interrogation signal duration, and not a

multiple of τ_d, the delay between adjacent taps. The length of the following tapped delay line L denotes the number of bits of the tag message. Each weight a_j is chosen to be either 0 or 1, representing the digit of the bit. Thus the RFID tag is able to transmit a total of $2^L - 1$ kinds of messages (the all 0-bit message is not used). The delay between adjacent taps τ_d must satisfy the condition $\tau_d \gg (\Delta\omega)^{-1}$ so as to reduce the interference between signals from adjacent delay taps. Delay τ_g is applied for the reason that if the RFID tag responds to the radar, the start bit (0-th bit) of the RFID tag's message always equals 1. Thus, the time interval between the start bit of the RFID tag's message and Correlator 1's output peak at the radar detector is τ_g, which can be used to verify and check the start of the RFID tag's message. Since we have ensured that τ_g is not a multiple of τ_d, the 0-th bit of the RFID tag's message will not be mistaken to be part of the RFID tag's actual message. Use of τ_g also guarantees that the RFID tag's message carrying the message sequence is distinct from the signal directly out of the bandpass filter, so that Correlator 2 of the radar detector can fully capture the RFID tag's message sequence after Correlator 1 detects whether the RFID tag responds or not.

The other branch of the bandpass filter output, which is used as the indicator of RFID tag message's arrival, goes directly to the amplifier and is retransmitted to the radar. Following this signal is the output of the weighted tapped delay line, which also goes through the amplifier and is transmitted back to the radar. Thus, the retransmitted signal for the i-th RFID tag has the vector form $\left[x_i(t) \quad x_i(t-\tau_g) + \sum_{j=1}^{L} a_j x_i(t-\tau_g - j\tau_d) \right]$.

2.3.3 Radar detector architecture

The radar detector functional block diagram is depicted in Figure 2.6. To detect the i-th RFID tag's message, the radar received signal $y(t)$ first goes through a bandpass filter whose frequency band corresponds to the i-th RFID tag. The bandpass filter selects the signal in the desired bandwidth, $y_i(t)$, and thus enhances the signal-to-noise ratio by eliminating out-of-band energy. The electronically controlled single-pole double-throw (SPDT) switch is always connected to Terminal 1 if it is not enabled. It switches to Terminal 2 only if it is enabled by the output of the threshold detector.

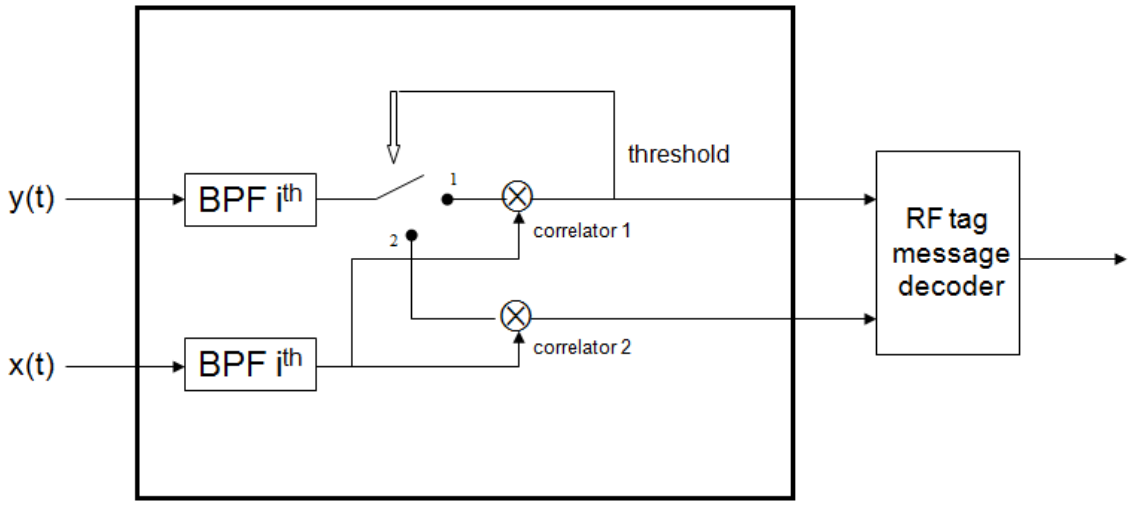


Figure 2.9. Radar detector block architecture.

The output of the bandpass filter $y_i(t)$ then goes to Correlator 1 where it is correlated with $x_i(t)$, a replica of the UWB noise radar signal saved at the radar filtered to the same band. Correlator 1 is used to detect $x_i(t)$, which is the initial portion of the RFID tag signal form. The integration time of Correlator 1 is T_1. If its output exceeds a threshold at some time, then it determines that the i-th RFID tag's message is coming in and triggers the SPDT switch. The

switch then switches to Terminal 2 and the remaining portion of the incoming signal $y_i(t)$ flows to Correlator 2.

Correlator 2 is used to decode the RFID tag's message. Compared to Correlator 1, Correlator 2 has a longer integration time, denoted by T_2, i.e. $T_2 > T_1$. The outputs of Correlator 1 and Correlator 2 both go to the RFID tag message decoder, which knows the length of the weighted tapped delay line of the RFID tag and the delay between its adjacent taps. By observing the amplitudes at different time lags, the RFID tag's message can be decoded. The output of Correlator 1 can help in decoding the RFID tag's message especially in the multipath channel case, which will be discussed in Chapter 3.

Delay τ_g is applied in our RFID tag design for the reason that if the RFID tag responds to the radar, the start bit (0-th bit) of the RFID tag's message always equals 1. Thus, the time interval between the start bit of the RFID tag's message and Correlator 1's output peak at the radar detector is τ_g, which can be used to verify and check the start of the RFID tag's message. Since clutter and RFID tag platforms will simply reflect the radar signal without the delay τ_g, reflections from these will be recognized as non-RFID tag. This enables discrimination by the radar between the RFID tag's signal and spurious reflections. Since we have ensured that τ_g is not a multiple of τ_d, the 0-th bit of the RFID tag's message will not be mistaken to be part of the RFID tag's actual message. The delay τ_g also guarantees that the RFID tag's message carrying signal sequence is separate from the signal direct out of the bandpass filter, so that Correlator 2 of the radar detector can fully capture the RFID tag's message sequence after Correlator 1 detects whether the RFID tag responds or not.

Figure 2.7 illustrates the structure of the correlator. The received signal is mixed with a time delayed version of the filtered transmitted signal $x_i(t-\tau)$. The correlation integration is

performed by the low-pass filter. The bandwidth of the low-pass filter determines the cross-correlation integration time.

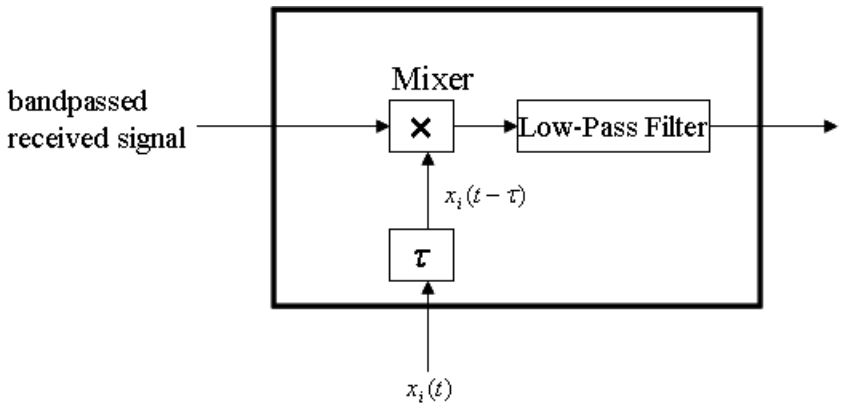


Figure 2.10. Structure of correlator.

When there are multiple RFID tags to be interrogated by the radar, several above detectors can be connected at the radar receiver in parallel, with each bandpass filter tuned to the corresponding RFID tag's center frequency.

Chapter 3

RFID tag — Radar system operation and performance analysis

3.1 System operation

We consider AWGN and propagation delays introduced by the channel. The internal thermal noise at the RFID tag and radar is neglected since it is much lower than the channel noise. We consider the link between the radar and RFID Tag 1 as an example to show the operation of the proposed system.

As stated before, to interrogate the RFID tags, the radar transmits the header $h(t)$ followed by the interrogation signal $x(t)$. If the RFID tag sensing receiver successfully captures the radar header, then the RFID tag responds to the radar with message modulated signals. Suppose the channel propagation delay is denoted by τ_0 and the channel additive noise in the radar-to-RFID tag link is denoted by $n_{f1}(t)$, then the output of the bandpass filter of the RFID tag is $x_1(t-\tau_0)+n_{f1}(t)$. The output of the weighted tapped delay line after power compensation by the amplifier is $x_1(t-\tau_g-\tau_0)+\sum_{j=1}^{L} a_j x_1(t-\tau_g-j\tau_d-\tau_0)+n_{f2}(t)$, where $n_{f2}(t)=n_{f1}(t-\tau_g)+\sum_{j=1}^{L} a_j n_{f1}(t-\tau_g-j\tau_d)$. Tag 1 thus transmits the signal $\left[\, x_1(t-\tau_0)+n_{f1}(t) \quad x_1(t-\tau_g-\tau_0)+\sum_{j=1}^{L} a_j x_1(t-\tau_g-j\tau_d-\tau_0)+n_{f2}(t) \,\right]$ back to the radar. Since the specific delay τ_g is only provided by the RFID tag, radar returns from clutter and RFID tag platforms will not introduce this delay, and thus their reflections will be discriminated from the

RFID tag's signal. In the following analysis, we ignore these unwanted radar returns assuming that they are fully separated from the RFID tag's signal at the radar detector.

At the radar receiver, the received signal after the bandpass filter $y_1(t)$ is given by

$$\begin{aligned} y_1(t) &= \begin{bmatrix} x_1(t-2\tau_0) + n_{f1}(t-\tau_0) + n_{b1}(t) \\ x_1(t-\tau_g-2\tau_0) + \sum_{j=1}^{L} a_j x_1(t-\tau_g - j\tau_d - 2\tau_0) + n_{f2}(t-\tau_0) + n_{b2}(t) \end{bmatrix} \\ &= \begin{bmatrix} x_1(t-2\tau_0) + n_1(t) \\ x_1(t-\tau_g-2\tau_0) + \sum_{j=1}^{L} a_j x_1(t-\tau_g - j\tau_d - 2\tau_0) + n_2(t) \end{bmatrix} \end{aligned} \tag{3.1}$$

where $n_{b1}(t)$ and $n_{b2}(t)$ are uncorrelated AWGN in the RFID tag-to-radar link. We also define $n_1(t) = n_{f1}(t-\tau_0) + n_{b1}(t)$ and $n_2(t) = n_{f2}(t-\tau_0) + n_{b2}(t)$.

The signals transmitted by other tags occupy different frequency bands, which do not overlap with the frequency band of the signal transmitted by the tag under consideration; thus the signals transmitted by other tags are uncorrelated with the desired signal. Therefore, the interference signals transmitted by other tags simply raise the noise floor at the radar detector corresponding to the tag under consideration. Furthermore, the guard band between individual tag frequency bands is designed to be much larger than the maximum Doppler frequency shift. The effect of such interferences on the system performance is equivalent to that of a degraded channel SNR.

The output of Correlator 1 is derived as

$$\begin{aligned} c_1(\tau) &= \int_0^{T_1} \left[x_1(t-2\tau_0) + n_1(t) \right] x_1(t-\tau) dt \\ &= \int_0^{T_1} x_1(t-2\tau_0) x_1(t-\tau) dt + \int_0^{T_1} n_1(t) x_1(t-\tau) dt \end{aligned} \tag{3.2}$$

Since $x_1(t)$ is uncorrelated with $n_1(t)$, the last term of equation (3.2) is a noise term. A peak whose magnitude is the energy of $x_1(t)$ should be observed at time lag $\tau = 2\tau_0$ of the Correlator 1 output, if RFID Tag 1's signal exists.

Similarly, the output of Correlator 2 is given by

$$c_2(\tau) = \int_0^{T_2} \left[x_1(t - \tau_g - 2\tau_0) + \sum_{j=1}^{L} a_j x_1(t - \tau_g - j\tau_d - 2\tau_0) + n_2(t) \right] x_1(t - \tau) dt$$
$$= \int_0^{T_2} x_1(t - \tau_g - 2\tau_0) x_1(t - \tau) dt + \sum_{j=1}^{L} a_j \int_0^{T_2} x_1(t - \tau_g - j\tau_d - 2\tau_0) x_1(t - \tau) dt + \int_0^{T_2} n_2(t) x_1(t - \tau) dt$$

(3.3)

To retrieve the RFID tag message, we need to observe the magnitude of the output of Correlator 2 at time lags $\tau = 2\tau_0 + \tau_g + j\tau_d \forall j = 1, \cdots L$. If a peak is observed at time lag when j equals l, then the l-th bit is 1, otherwise it is 0.

To demonstrate on paper the operation of the RFID tag responding system, we ran simulations on the following example.

A 4th order bandpass Chebyshev filter with 0.5 dB ripple in the passband is used for the simulation, whose frequency response is shown in Figure 3.1. The radar transmits a 1–2 GHz noise signal to the RFID tags. The ratio of the durations of the radar header to the radar inquiry signal part is 1:5. To illustrate the operation of the proposed system, suppose that there are three RFID tags within the radar's range. The RFID tags' operating bandwidth is 320 MHz and their frequency band allocation is as follows: Tag 1 occupies 1–1.32 GHz, Tag 2 occupies 1.34–1.66 GHz, and Tag 3 occupies 1.68–2 GHz. The guard bandwidth is 20 MHz, which is much greater than what is needed to account for the tag's maximum possible Doppler shift. The channel SNR is −3 dB, and the channel round propagation delay is 1.6×10^4 time lags. The length of the

weighted tapped delay line at the RFID tag is 3. The delay between adjacent taps, τ_d, is 90 time lags, and the delay before the tapped delay line, τ_g, is 5030 time lags, which is longer than the radar interrogation signal duration of 5000 time lags. RFID Tag 1 transmits message 101 to the radar, i.e. using delays τ_d and $3\tau_d$.

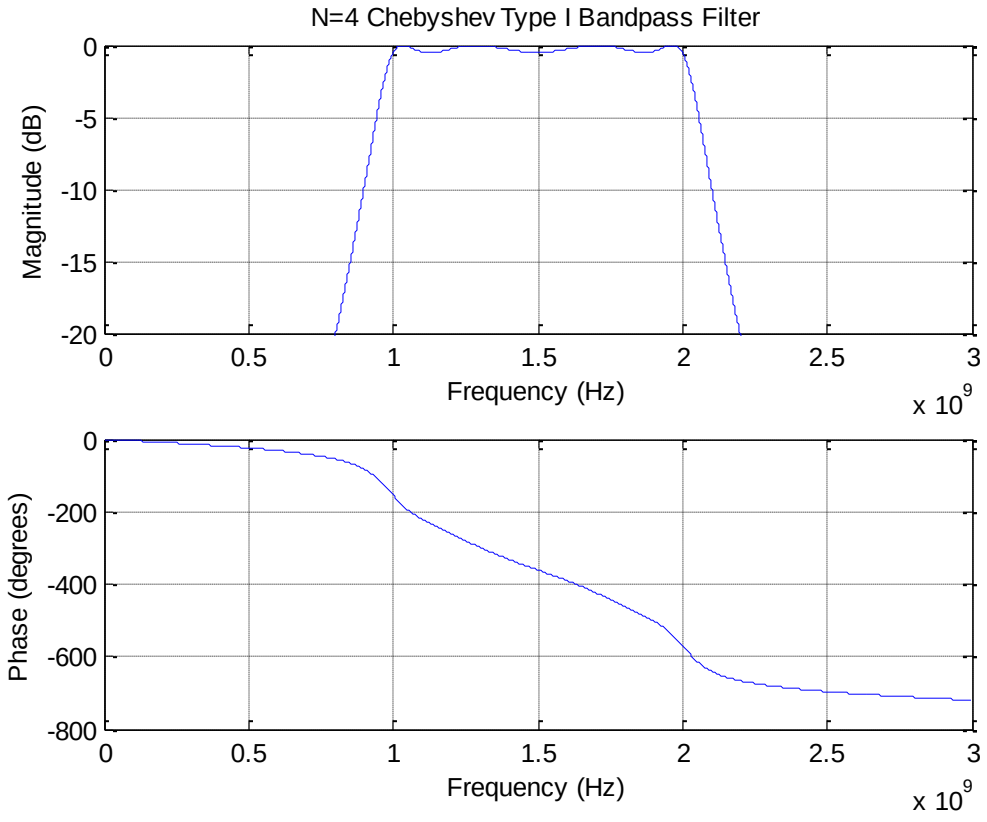


Figure 3.1. Frequency response of bandpass filter at the radar transmitter output.

Figure 3.2 shows the simulation results of RFID Tag 1's message decoding in the AWGN channel case in the example system. The output of Correlator 1 has a peak at the time lag of 1.6×10^4, which indicates that a message from RFID Tag 1 exists. In the output of Correlator 2, a peak occurs at the time lag around 21030, which indicates the start of the RFID tag's message. Subsequent two peaks occur at 90 time lags and 270 time lags, which equal τ_d and $3\tau_d$

respectively away from the start of the message. There is no peak occurring at 180 time lags corresponding to $2\tau_d$. Thus, this RFID tag's message is correctly interpreted as 101.

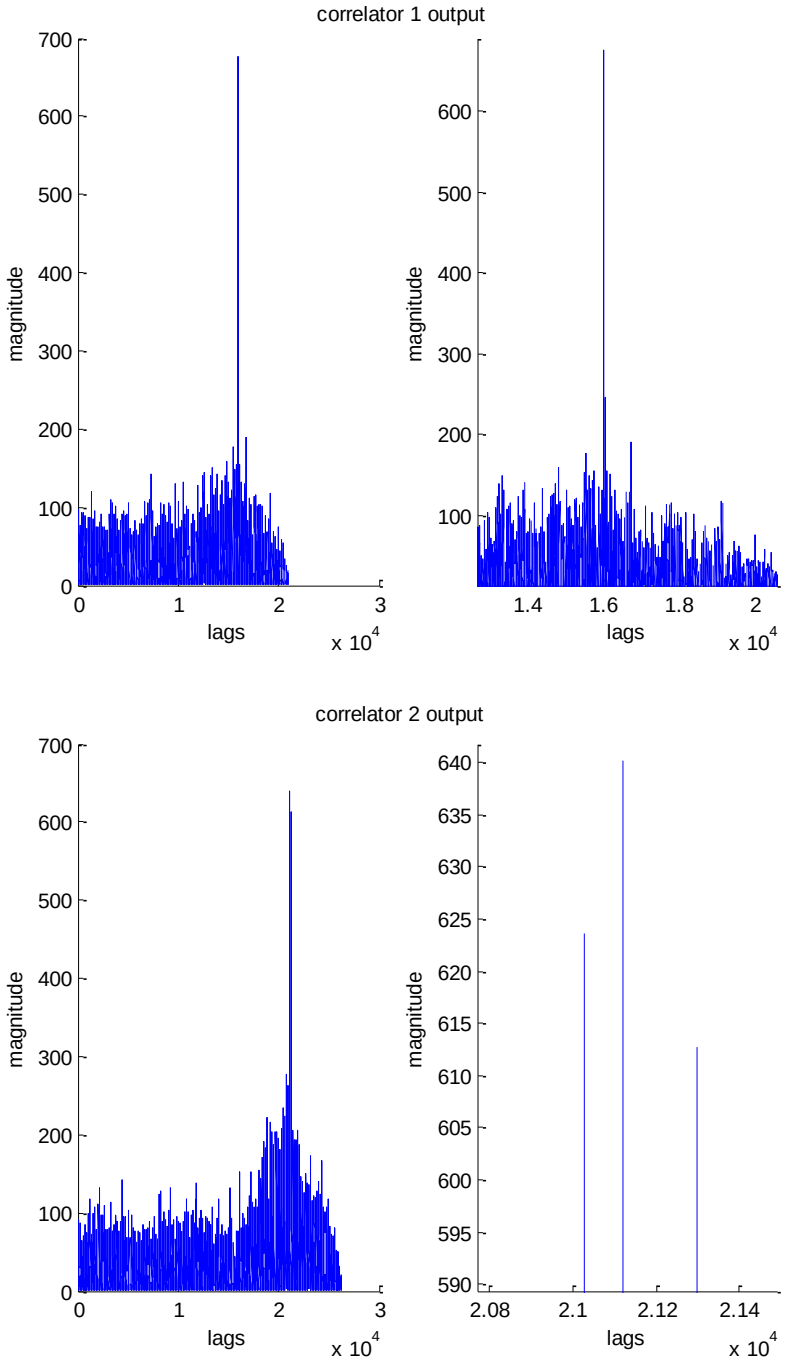


Figure 3.2. Example system RF tag message decoding in AWGN channel at an SNR value of −3 dB. The right plots are zoomed in at the peaks of the left plots.

3.2 System performance analysis

The performance of the system is evaluated in term of the symbol error probability, also known as the symbol error ratio (SER). As stated above, interferences such as clutter reflections and other RFID tags' transmitted signals can be either discriminated from the desired signals at the radar decoder or can be analyzed as being equivalent to a worse channel SNR. In the following analysis, we derive the SER of our system in an AWGN channel to give a theoretical bound that our system can best achieve. Whether the RFID tag's message can be correctly decoded or not depends on the outputs of both the Correlator 1 and Correlator 2. The RFID tag header has to be detected at first.

The output of Correlator 1 gives an indication whether this RFID tag responds to the radar. The zeroth bit of the RFID tag's message (when it exists) is always 1, and since τ_g is not a multiple of τ_d, it will not be misconstrued as part of the tag message. If the peak of Correlator 1's output appears at time τ_x, which may be different from $2\tau_0$ due to factors such as the delay caused by processing time of components in reality, and the first peak of Correlator 2's output appears at time τ_y, then the time interval between τ_x and τ_y will equal τ_g. This way, the start of the RFID tag's message can be checked and verified.

The RFID tag message decoding rule is that if no peak of Correlator 1's output appears at any time, then the RFID tag's message is wrongly decoded; else if the peak of Correlator 1's output appears at some time τ_x, then if no peak appears at time around τ_g away from τ_x, then the RFID tag's message is wrongly decoded; else the RF tag's message is decoded by observing the magnitude of Correlator 2' s output at time $\tau_g + j\tau_d \forall j = 1, \cdots L$ away from τ_x.

Therefore, the symbol error probability can be written as

$$
\begin{aligned}
p_s(e) &= p(\bar{c}_1) + p(c_1)\left(p(\bar{c}_{2g}) + p(c_{2g})\left(1 - \prod_{k=1}^{L}(1 - p(\bar{c}_{2k}))\right)\right) \\
&= p(\bar{c}_1) + \left(1 - p(\bar{c}_1)\right)\left(p(\bar{c}_{2g}) + \left(1 - p(\bar{c}_{2g})\right)\left(1 - \prod_{k=1}^{L}(1 - p(\bar{c}_{2k}))\right)\right)
\end{aligned}
\tag{3.4}
$$

where $p(\bar{c}_1)$ is the probability that Correlator 1 gives a wrong decision, $p(\bar{c}_{2g})$ is the probability that a wrong decision is made at time τ_g away from τ_x of Correlator 2's output in case that Correlator 1 gives a correct decision, and $p(\bar{c}_{2k})$ represents the probability of the k-th bit of RFID tag's message decoded wrongly given that Correlator 1 gives a correct decision as well as the 0-th bit is correctly decoded.

The probability $p(\bar{c}_1)$ that Correlator 1 gives a wrong indication is calculated as follows. Although the peak may appear at time other than $2\tau_0$, the derived result is still applicable since we use the ideal time $2\tau_0$ merely to show the calculation procedure for the time where the peak of Correlator 1's output should occur. The peak output is given by

$$
\begin{aligned}
c_1(2\tau_0) &= \int_0^{T_1}\left[a_{c1}x_1(t-2\tau_0) + n_1(t)\right]x_1(t-2\tau_0)dt \\
&= a_{c1}\int_0^{T_1} x_1^2(t-2\tau_0)dt + \int_0^{T_1} n_1(t)x_1(t-2\tau_0)dt \\
&= a_{c1}U_{x11} + n_{e1}(t)
\end{aligned}
\tag{3.5}
$$

where the coefficient a_{c1} is either 1 or 0 corresponding to whether the RFID tag responds to the radar or not. Upon invoking the stationarity property for $x_1(t)$, we have

$$
U_{x11} = \int_0^{T_1} x_1^2(t-2\tau_0)dt = \int_0^{T_1} x_1^2(t)dt\,, \tag{3.6}
$$

while

$$
n_{e1}(t) = \int_0^{T_1} n_1(t)x_1(t-2\tau_0)dt \tag{3.7}
$$

represents the noise term. A simulation check confirms that we can approximate $n_{e1}(t)$ as Gaussian distributed.

Since $n_1(t) = n_{f1}(t-\tau_0) + n_{b1}(t)$, and $n_{f1}(t-\tau_0)$ and $n_{b1}(t)$ are uncorrelated Gaussian noise, both with zero mean and variance σ_n^2, the mean of $n_1(t)$ is zero and its variance is $2\sigma_n^2$. The mean of $n_{e1}(t)$ is zero, and its variance is computed as

$$\begin{aligned}
\mathrm{Var}\{n_{e1}(t)\} &= \mathrm{E}\left\{n_{e1}(t)^2\right\} \\
&= \mathrm{E}\left\{\int_0^{T_1} n_1(t)x_1(t-2\tau_0)dt \int_0^{T_1} n_1(t')x_1(t'-2\tau_0)dt'\right\} \\
&= \int_0^{T_1}\int_0^{T_1} \mathrm{E}\left\{n_1(t)x_1(t-2\tau_0)n_1(t')x_1(t'-2\tau_0)dtdt'\right\} \\
&= \int_0^{T_1} \mathrm{E}\left\{n_1(t)^2\right\}\cdot\mathrm{E}\left\{x_1(t-2\tau_0)^2\right\}dt \\
&= T_1\sigma_{n1}^2\sigma_{x1}^2 \\
&= 2T_1\sigma_n^2\sigma_{x1}^2
\end{aligned} \tag{3.8}$$

Since $n_1(t)$ and $x_1(t)$ are white Gaussian noise signals, each is uncorrelated to its time delayed replica.

The signal component of $c_1(2\tau_0)$ is either 0 or U_{x11}. The possibility whether the branch of signal out of the bandpass filter at the RFID tag is sent out directly to the radar depends on many factors, such as whether it can successfully capture the radar header, its power condition since we use active RFID tags in the system, etc. For simplicity, we assume that each value is equally probable. The optimal threshold can be shown to be

$$\chi_1 = \frac{1}{2}U_{x11} \tag{3.9}$$

The noise variance is σ_{e1}^2 which can be shown to be equal to the power spectral density $N_0/2$ for a white Gaussian process. The distance d_{12} between the two signal values is U_{x11}. The average probability of error is calculated to be [48]

$$P(\bar{c}_1) = Q\left[\sqrt{\frac{d_{12}^2}{2N_0}}\right] = Q\left[\frac{1}{2}\frac{U_{x11}}{\sigma_{e1}}\right] = Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{2T_1}\sigma_n\sigma_{x1}}\right] \tag{3.10}$$

where the Q-function is given by $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt, \ x \geq 0$.

If Correlator 1 at the radar receiver correctly detects the existence of the RFID tag signal, we need to check whether the 0-th bit of RFID tag's message exists or not. The output of Correlator 2 at the corresponding time is given by

$$\begin{aligned} c_2(2\tau_0 + \tau_g) &= \int_0^{T_2} \left[x_1(t - \tau_g - 2\tau_0) + \sum_{j=1}^{L} a_j x_1(t - \tau_g - j\tau_d - 2\tau_0) + n_2(t) \right] x_1(t - 2\tau_0 - \tau_g) dt \\ &= \int_0^{T_2} x_1^2(t - \tau_g - 2\tau_0) dt + \sum_{j=1}^{L} a_j \int_0^{T_2} x_1(t - \tau_g - j\tau_d - 2\tau_0) x_1(t - \tau_g - 2\tau_0) dt + \\ &\quad \int_0^{T_2} n_2(t) x_1(t - \tau_g - 2\tau_0) dt \\ &= \int_0^{T_2} x_1^2(t - \tau_g - 2\tau_0) dt + n_{eg} \end{aligned} \tag{3.11}$$

where

$$\int_0^{T_2} x_1^2(t - \tau_g - 2\tau_0) dt = \int_0^{T_1} x_1^2(t) dt = U_{x11} \tag{3.12}$$

is the signal component and

$$n_{eg} = \sum_{j=1}^{L} a_j \int_0^{T_2} x_1(t - \tau_g - j\tau_d - 2\tau_0) x_1(t - \tau_g - 2\tau_0) dt + \int_0^{T_2} n_2(t) x_1(t - \tau_g - 2\tau_0) dt \tag{3.13}$$

denotes the noise term.

Since $\tau_d \gg (\Delta\omega)^{-1}$, the signals out of different delay taps at the RFID tag can be considered as uncorrelated. Thus the components of $n_{eg}(t)$ are pairwise uncorrelated, and each component can be approximated as Gaussian distributed, so they are independent. Then, $n_{eg}(t)$ can be approximated as Gaussian distributed with mean zero and variance σ_{eg}^2. The variance of

$n_{eg}(t)$ is the sum of the variances of each component. Following the same procedure as in (3.8), its variance is calculated to be

$$\sigma_{eg}^2 = \sum_{j=1}^{L} a_j T_2 \sigma_{x1}^4 + T_2 \sigma_{n2}^2 \sigma_{x1}^2 \tag{3.14}$$

Since $n_2(t) = n_{f2}(t-\tau_0) + n_{b2}(t)$ and $n_{f2}(t) = n_{f1}(t-\tau_g) + \sum_{j=1}^{L} a_j n_{f1}(t-\tau_g - j\tau_d)$,

where $n_{f1}(t-\tau_g)$ is uncorrelated with $n_{b2}(t)$, we have

$$\sigma_{n2}^2 = \sigma_n^2 + \sigma_n^2(1+\sum_{j=1}^{L} a_j) \tag{3.15}$$

Therefore,

$$\begin{aligned} \sigma_{eg}^2 &= \sum_{j=1}^{L} a_j T_2 \sigma_{x1}^4 + T_2(\sigma_n^2 + \sigma_n^2(1+\sum_{j=1}^{L} a_j))\sigma_{x1}^2 \\ &= T_2 \sigma_{x1}^2 \left[\sigma_{x1}^2 \sum_{j=1}^{L} a_j + \sigma_n^2(2+\sum_{j=1}^{L} a_j) \right] \end{aligned} \tag{3.16}$$

Similarly as in the analysis for $p(\bar{c}_1)$, the signal component of $c_2(2\tau_0 + \tau_g)$ which may be 0 or U_{x11}, is assumed to be equally probable, and so

$$\begin{aligned} p(\bar{c}_{2g}) &= Q\left[\frac{1}{2} \frac{U_{x11}}{\sigma_{eg}} \right] \\ &= Q\left[\frac{1}{2} \frac{U_{x11}}{\sqrt{T_2}\sigma_{x1} \sqrt{\sigma_{x1}^2 \sum_{j=1}^{L} a_j + \sigma_n^2(2+\sum_{j=1}^{L} a_j)}} \right] \end{aligned} \tag{3.17}$$

Given that Correlator 1 gives a correct decision as well as the 0-th bit is correctly decoded, to determine the k -th bit, we observe the amplitude of Correlator 2's output at time lag $2\tau_0 + \tau_g + k\tau_d$. The output at the corresponding time lag is given by

$$\begin{aligned} c_2(2\tau_0 + \tau_g + k\tau_d) &= \int_0^{T_2} \left[x_1(t - \tau_g - 2\tau_0) + \sum_{j=1}^{L} a_j x_1(t - \tau_g - j\tau_d - 2\tau_0) + n_2(t) \right] x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt \\ &= \int_0^{T_2} x_1(t - \tau_g - 2\tau_0) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt + \\ &\quad a_k \int_0^{T_2} x_1^2(t - 2\tau_0 - \tau_g - k\tau_d) dt + \\ &\quad \sum_{j=1, j\neq k}^{L} a_j \int_0^{T_2} x_1(t - 2\tau_0 - \tau_g - j\tau_d) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt + \\ &\quad \int_0^{T_2} n_2(t) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt \\ &= a_k \int_0^{T_2} x_1^2(t - 2\tau_0 - \tau_g - k\tau_d) dt + n_{e2}(t) \end{aligned} \tag{3.18}$$

where

$$\int_0^{T_2} x_1^2(t - 2\tau_0 - \tau_g - k\tau_d) dt = U_{x11} \tag{3.19}$$

and $n_{e2}(t)$ represents the noise terms, given by

$$\begin{aligned} n_{e2}(t) &= \int_0^{T_2} x_1(t - \tau_g - 2\tau_0) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt + \\ &\quad \sum_{j=1, j\neq k}^{L} a_j \int_0^{T_2} x_1(t - 2\tau_0 - \tau_g - j\tau_d) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt + \\ &\quad \int_0^{T_2} n_2(t) x_1(t - 2\tau_0 - \tau_g - k\tau_d) dt \end{aligned} \tag{3.20}$$

Similarly, we can show that $n_{e2}(t)$ can be approximated as Gaussian distributed with mean zero and variance σ_{e2}^2. Following the same procedure as in (3.8), the variance of $n_{e2}(t)$ is calculated to be

$$\begin{aligned}\sigma_{e2}^2 &= T_2\sigma_{x1}^2[\sigma_{x1}^2 + \sigma_{x1}^2\sum_{j=1,\,j\neq k}^{L} a_j + \sigma_{n2}^2] \\ &= T_2\sigma_{x1}^2\left[\sigma_{x1}^2 + \sigma_{x1}^2\sum_{j=1,\,j\neq k}^{L} a_j + \sigma_n^2\left(2+\sum_{j=1}^{L} a_j\right)\right]\end{aligned} \tag{3.21}$$

The signal component of $c_2(2\tau_0 + \tau_g + k\tau_d)$ is either 0 or U_{x11} since the coefficient a_k is either 0 or 1. Assuming that each value is equally probable, the optimal threshold in this case is then

$$\chi_2 = \frac{1}{2}U_{x11} \tag{3.22}$$

The average probability of error for the k-th bit of the RFID tag's message is given by

$$\begin{aligned}p(\bar{c}_{2k}) &= Q\left[\frac{1}{2}\frac{U_{x11}}{\sigma_{e2}}\right] \\ &= Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{T_2}\sigma_{x1}\sqrt{\sigma_{x1}^2 + \sigma_{x1}^2\sum_{j=1,\,j\neq k}^{L} a_j + \sigma_n^2\left(2+\sum_{j=1}^{L} a_j\right)}}\right]\end{aligned} \tag{3.23}$$

Substituting (3.10), (3.17), and (3.23) into (3.4), we derive the symbol error probability (SER) as

$$
\begin{aligned}
p_s(e) = {} & Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{2T_1}\sigma_n\sigma_{x1}}\right] + \\
& \left(1 - Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{2T_1}\sigma_n\sigma_{x1}}\right]\right)\times \\
& \left(Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{T_2}\sigma_{x1}\sqrt{\sigma_{x1}^2\sum_{j=1}^{L}a_j + \sigma_n^2(2+\sum_{j=1}^{L}a_j)}}\right] + \right. \\
& \left(1 - Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{T_2}\sigma_{x1}\sqrt{\sigma_{x1}^2\sum_{j=1}^{L}a_j + \sigma_n^2(2+\sum_{j=1}^{L}a_j)}}\right]\right)\times \\
& \left.\left(1 - \prod_{k=1}^{L}\left(1 - Q\left[\frac{1}{2}\frac{U_{x11}}{\sqrt{T_2}\sigma_{x1}\sqrt{\sigma_{x1}^2 + \sigma_{x1}^2\sum_{j=1,j\neq k}^{L}a_j + \sigma_n^2\left(2+\sum_{j=1}^{L}a_j\right)}}\right]\right)\right)\right)
\end{aligned}
\tag{3.24}
$$

As can be seen from (3.13) and (3.20), when the RFID tag transmits all 1-bit messages, the noise floor is higher than when it transmits other kinds of messages. Thus, the worst SER is obtained for this case.

We ran simulations on the proposed system's SER using the same example system as that for system operation illustration. The RFID tag has a 3-tapped delay line, where the delay between adjacent taps is 90 time lags, and the delay before the tapped delay line at the RFID tag is 5030 time lags. The round propagation delay is 16000 time lags. Radar transmits a 1−2 GHz noise signal towards the RFID tag, and the RFID tag signal occupies the 1−1.32 GHz band. In Figure 3.3, simulation results of the SER are shown as a function of the channel signal-to-noise ratio (SNR), and it is compared to the theoretical result derived from (3.24).

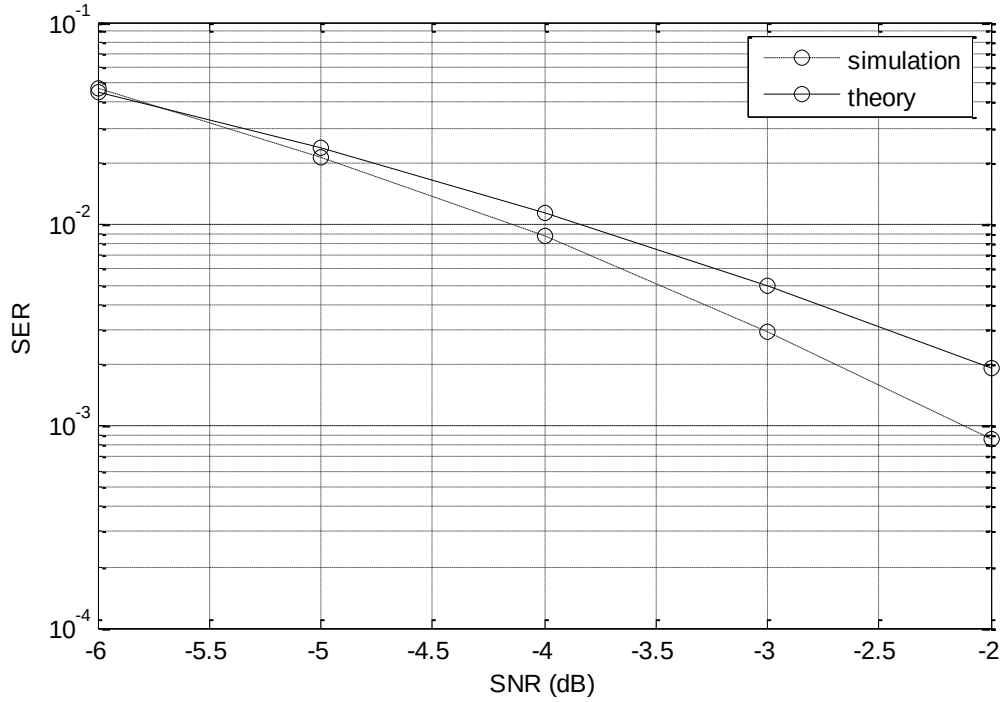


Figure 3.3. Example system SER vs. channel SNR for a 3-tap delay line at the RFID tag.

We note from Figure 3.3 that the simulation and theoretical results agree to within 0.5 dB. The simulation and theoretical results show that the proposed system is capable of covertly and securely communicating messages even under negative channel SNR conditions with tolerable symbol error probability. When the channel SNR is −2 dB, the SER of the system is at the 10^{-3} level, and the system still performs well at –4 dB channel SNR, where the SER is at the 10^{-2} level. Figure 3.3 also reveals that the theoretical curve slightly overestimates the SER at a given channel SNR compared to the simulation results, but the agreement is within 0.7 dB over the range investigated. The simulated and theoretically derived SER curves do not match exactly due to the fact that in our SER derivation, we approximate the distribution of the noise term out of the correlator as Gaussian to obtain a closed form solution. However, since this noise term also contains products of Gaussian random variables, it is not strictly Gaussian distributed, according to [49].

3.3 RFID tag-to-Radar link multipath interferences reduction

Since the RFID tag's message is modulated to the signal through weighted tapped delays, when there are multipath interferences in the RFID tag-to-radar link, the RFID tag multipath signals appearing at various times may confuse the tag's message decoding at the radar. Thus, the multipath interferences need to be reduced at the radar before determining the tag's message. In this section, an algorithm to reduce the interferences from multipath signals in the RFID tag-to-radar link is presented, and illustrated through simulation. This algorithm is specifically designed for our system wherein we use random noise signal as the information carrier. We developed this algorithm considering both the complexity of the system, especially the simple architecture of the RFID tag, and the fact that the system can work in real time, as long as assuming the multipath channel remains relatively constant over the duration of tag operation. Our simulation results show that this algorithm works for the proposed system.

3.3.1 Multipath interferences reduction procedure

The basic idea is that the signal from the branch directly out of the bandpass filter at the RFID tag can also be used to sense the multipath channel on the RFID tag-to-radar link during the detection by the radar when determining whether the corresponding RFID tag is responding. The multipath channel information thus estimated is applied to the following sequence of signals to reduce the interferences brought about by the multipath signals, and to better decode the RFID tag's message by the radar.

IEEE 802.15.4a has provided channel models describing signal propagation over 3.1–10.6 GHz for various environments, such as indoor residential, indoor office, industrial environments, etc. The set of IEEE multipath channel models is based on the Saleh-Valenzuela

model, where the paths arrive at the receiver in clusters. To demonstrate how our proposed scheme combats multipath signal interferences, we use a more simplified channel model.

Consider the RFID tag-to-radar link. The multipath channel response is simply modeled by a finite set of delay and attenuation pairs $\{\alpha_i, \tau_{mi}\}$,

$$h_m(t) = \sum_{i=1}^{M} \alpha_i \delta(t - \tau_{mi}) \tag{3.25}$$

The radar received signal out of the bandpass filter which flows to Correlator 1 is given by

$$\begin{aligned} x_{1c1}(t) &= h_m(t) \otimes \left[x_1(t - 2\tau_0) + n_{f1}(t - \tau_0) \right] + n_{b1}(t) \\ &= \sum_{i=1}^{M} \alpha_i x_1(t - 2\tau_0 - \tau_{mi}) + \sum_{i=1}^{M} \alpha_i n_{f1}(t - \tau_0 - \tau_{mi}) + n_{b1}(t) \\ &= \sum_{i=1}^{M} \alpha_i x_1(t - 2\tau_0 - \tau_{mi}) + n_{m1}(t) \end{aligned} \tag{3.26}$$

where $n_{m1}(t) = \sum_{i=1}^{M} \alpha_i n_{f1}(t - \tau_0 - \tau_{mi}) + n_{b1}(t)$ represents the noise term of $x_{1c1}(t)$.

Similarly, the branch of the radar bandpass filter to Correlator 2 is given by

$$\begin{aligned} x_{1c2}(t) &= h_m(t) \otimes \left[x_1(t - \tau_g - 2\tau_0) + \sum_{j=1}^{L} a_j x_1(t - \tau_g - j\tau_d - 2\tau_0) + n_{f2}(t - \tau_0) \right] + n_{b2}(t) \\ &= \sum_{i=1}^{M} \alpha_i x_1(t - 2\tau_0 - \tau_g - \tau_{mi}) + \\ &\quad \sum_{j=1}^{L} a_j \sum_{i=1}^{M} \alpha_i x_1(t - \tau_g - 2\tau_0 - j\tau_d - \tau_{mi}) + \\ &\quad \sum_{i=1}^{M} \alpha_i n_{f2}(t - \tau_0 - \tau_{mi}) + n_{b2}(t) \\ &= \sum_{i=1}^{M} \alpha_i x_1(t - 2\tau_0 - \tau_g - \tau_{mi}) + \sum_{j=1}^{L} a_j \sum_{i=1}^{M} \alpha_i x_1(t - \tau_g - 2\tau_0 - j\tau_d - \tau_{mi}) + n_{m2}(t) \end{aligned} \tag{3.27}$$

where $n_{m2}(t) = \sum_{i=1}^{M} \alpha_i n_{f2}(t - \tau_0 - \tau_{mi}) + n_{b2}(t)$ represents the noise term of $x_{1c2}(t)$.

The output of Correlator 1 is calculated as

$$\begin{aligned} c_1(\tau) &= \int_0^{T_1} x_{1c1}(t) x_1(t-\tau) dt \\ &= \sum_{i=1}^{M} \alpha_i \int_0^{T_1} x_1(t - 2\tau_0 - \tau_{mi}) x_1(t-\tau) dt + \int_0^{T_1} n_{m1}(t) x_1(t-\tau) dt \end{aligned} \tag{3.28}$$

The output of Correlator 2 output is calculated as

$$\begin{aligned} c_2(\tau) &= \int_0^{T_1} x_{1c2}(t) x_1(t-\tau) dt \\ &= \sum_{i=1}^{M} \alpha_i \int_0^{T_2} x_1(t - 2\tau_0 - \tau_g - \tau_{mi}) x_1(t-\tau) dt + \\ &\sum_{j=1}^{L} a_j \sum_{i=1}^{M} \alpha_i \int_0^{T_2} x_1(t - \tau_g - 2\tau_0 - j\tau_d - \tau_{mi}) x_1(t-\tau) dt + \\ &\int_0^{T_2} n_{m2}(t) x_1(t-\tau) dt \end{aligned} \tag{3.29}$$

If the output of Correlator 1 has a peak above the threshold at some time lag τ^*, then the radar starts to decode this RFID tag's message with the outputs of Correlator 2, $c_2(\tau)$, and Correlator 1, $c_1(\tau)$.

The first step of tag message decoding is to suppress the noise floor of $c_1(\tau)$ and $c_2(\tau)$. We denote $c_1'(\tau)$ and $c_2'(\tau)$ as the denoised versions of $c_1(\tau)$ and $c_2(\tau)$, respectively. The noise can be reduced using the method of wavelets. The energy of a signal is often concentrated in a few coefficients, while the energy of noise is spread among all coefficients in the wavelet domain [50]. Wavelet denoising keeps strong wavelet components and removes the rest, and as a result, the noise is removed according to the signal [51]. Wavelet denoising has the merit of optimal resolution both in the time and the frequency domain compared to other methods [52], and it is therefore widely used for noise reduction purposes. The denoising procedure consists of three

stages: (1) wavelet transformation of the signal; (2) thresholding of wavelet coefficients; and (3) inverse wavelet transformation [53]. One threshold ξ that is easy to implement is given by [54]

$$\xi = \sigma\sqrt{(2\log n)/n}\,, \tag{3.30}$$

where n is the number wavelet coefficients to be thresholded and $\sigma = \tilde{m}/0.6745$, $\tilde{m}$ being the median of the wavelet transform coefficients.

The next step is to apply the information obtained from $c_1'(\tau)$ to $c_2'(\tau)$ in order to decode the RFID tag message. The procedure is described as follows:

STEP 1: Intercept the part of $c_1'(\tau)$ from time lag τ^*, which is denoted as $c_{1r}'(\tau)$.

STEP 2: Check the 0-th bit of the RFID tag's message by observing the magnitude of $c_2'(\tau)$ at time lag $\tau^* + \tau_g$. If it is above the threshold, then go to STEP 3, otherwise stop.

STEP 3: Intercept the part of $c_2'(\tau)$ from time lag $\tau^* + \tau_g$, denoted as $c_{2\_0}'(\tau)$. Subtract $c_{1r}'(\tau)$ from $c_{2\_0}'(\tau)$, and the remaining part is denoted as $c_{20}'(\tau)$. Check the 1st bit of the RFID tag's message by observing the magnitude of $c_{20}'(\tau)$ at time lag $\tau_g + \tau_d$ away from τ^*. If it is above the threshold, then the first bit is decoded as 1, and go to STEP 4. Otherwise the first bit is decoded as 0, and check from the next bit.

STEP 4: Intercept the part of $c_{20}'(\tau)$ from time lag $\tau^* + \tau_g + \tau_d$, denoted as $c_{2\_1}'(\tau)$. Subtract $c_{1r}'(\tau)$ from $c_{2\_1}'(\tau)$, and the remaining part is denoted as $c_{21}'(\tau)$.

……

STEP 5: Repeat the above operation on the resulting signal iteratively at time lag $\tau^* + \tau_g + i \cdot \tau_d$ for all $i = 1, 2, \ldots, L$.

3.3.2 Test channel

The channel impulse response used in the simulation is shown in Figure 3.4, which although not a standard one, is just for algorithm testing and validation purposes.

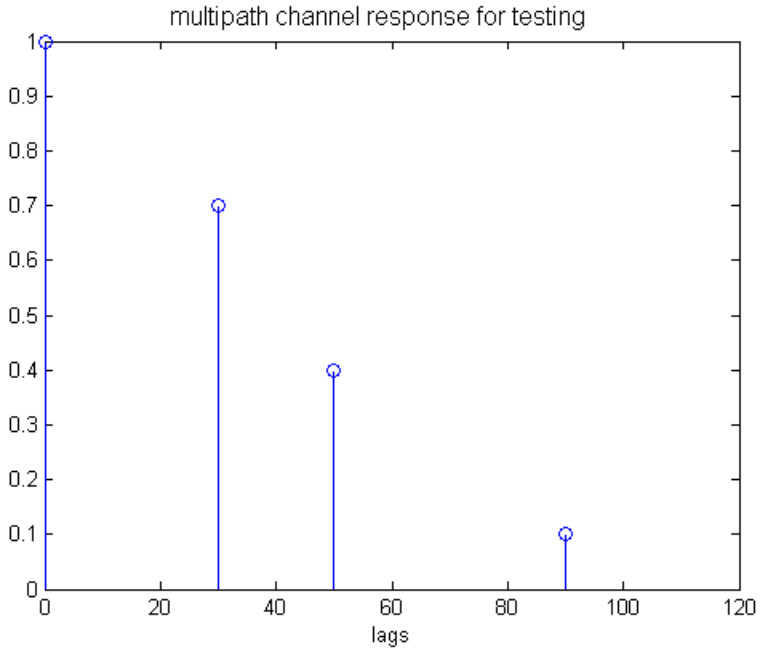
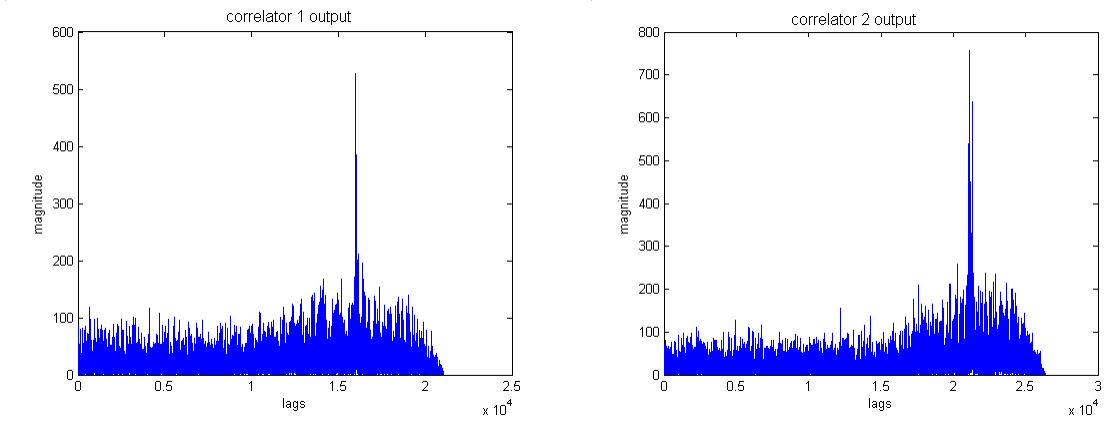


Figure 3.4. Channel impulse response used for testing.

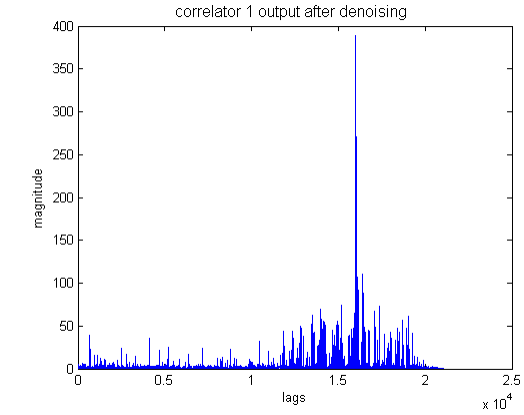
3.3.3 Multipath interferences reduction results

The following is a simulation validation for the proposed method. We use the same system example as that in Section 3.1, except that the channel is changed. The channel impulse response used in the simulation is shown in Figure 3.4. The wavelet used in the test is the Daubechies-4 (db4) wavelet, a widely used wavelet for signal processing [55]. The simulation results are shown in Figures 3.5(a)-(h). Figures 3.5(a) and 3.5(b) show the correlator outputs wherein the multipath signals and significant amount of noise are shown. The correlator outputs after denoising as per the procedure outlined in Equation (3.30) are shown in Figures 3.5(c) and

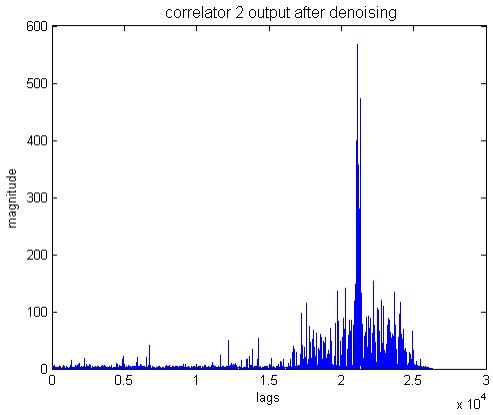
3.5(d), wherein we note that noise has significantly reduced. Figure 3.5(e) shows the output of Correlator 2 after the first multipath signal removal. An enlarged view of the Correlator 2's output after the first multipath signal removal is presented in Figure 3.5(f), which shows a high peak value at around 90 lags, which equals τ_d away from where the 0-th bit appears; thus the first bit is decoded as 1. In Figure 3.5(g), Correlator 2's output after the second multipath signal removal shows that there is no high peak value observed at 180 lags which equals $2\tau_d$ away from where the 0-th bit appears, so the second bit is decoded as 0. However, there exists a high peak value occurring at about 270 lags which equals $3\tau_d$ away from where the 0-th bit appears, so the third bit is determined as 1. Since the length of the delay line at the RFID tag is known by the radar, the message is interpreted as 101 by the radar. Figure 3.5(h) shows the output of Correlator 2 after three multipath signal removal iterations. It shows that the multipath interferences are reduced significantly.



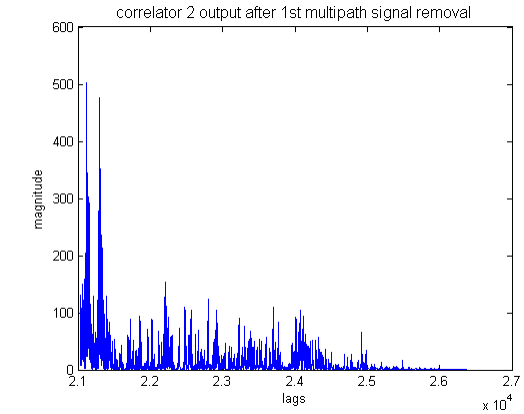
(a) (b)


correlator 1 output after denoising
magnitude
lags
x 10^4

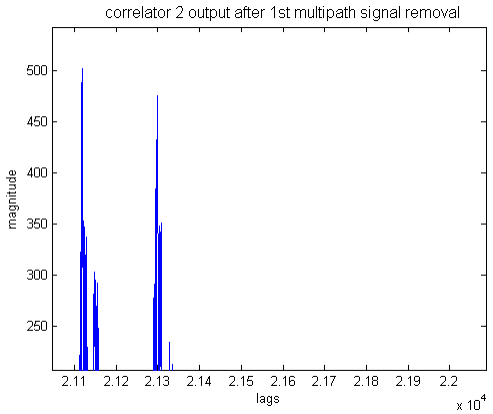
(c)


correlator 2 output after denoising
magnitude
lags
x 10^4

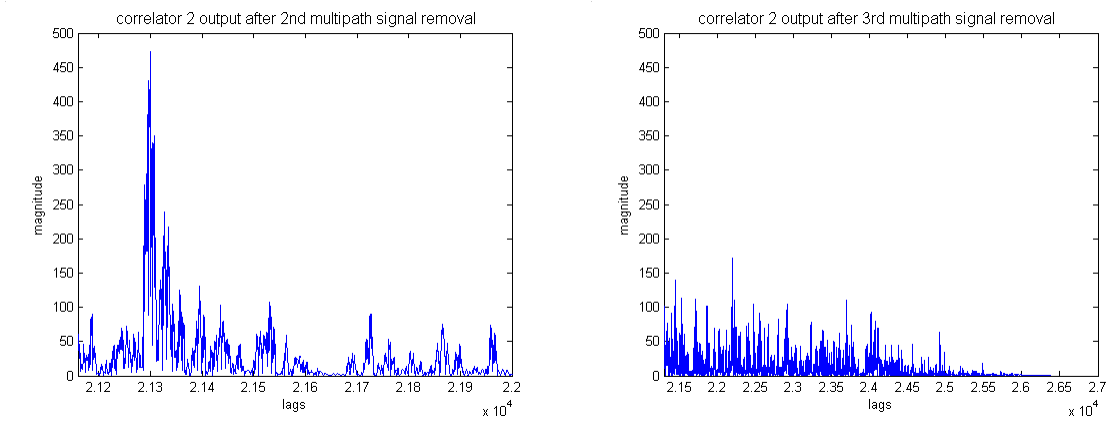
(d)


correlator 2 output after 1st multipath signal removal
magnitude
lags
x 10^4

(e)


correlator 2 output after 1st multipath signal removal
magnitude
lags
x 10^4

(f)



(g) (h)

Figure 3.5 Example system multipath channel results. (a) Correlator 1 output in multipath channel case, (b) Correlator 2 output in multipath channel case, (c) Correlator 1 output after noise suppression, (d) Correlator 2 output after noise suppression, (e) RFID tag message decoding after the 1st multipath signal removal iteration, (f) Same as (e) with lag scale expanded, (g) RFID tag message decoding after the 2nd multipath signal removal iteration, (h) RFID tag message after the 3rd multipath signal removal iteration.

In the multipath channel, there will also be multipath from radar to the RFID tag. The radar-to-RFID tag channel and the RFID tag-to-radar channel are likely to be different given that both systems will have different antenna patterns. As stated in the RFID tag architecture in Section 2.3.2, our design of the sleep mode in RFID tag's operation assures that during one radar inquiry, once the RFID is triggered, it will not be triggered by multipath signals.

3.4 System implementation considerations

Various mature technologies, e.g., microwave, photonic, and acousto-optic, can be implemented to realize the switchable delay lines at the RFID tag for transmitting different messages, as described in [56]–[60]. A variable photonic microwave delay line and a spatially

integrated optic implementation are presented in [56]. An L-hand 5 bit time shifter is developed in [58], using switched diode lasers and photo detectors in conjunction with fiber-optic delay lines. An electrically tunable true-time-delay line in silicon for a broadband noise radar is described in [59], which consists of discrete switchable lines realized in hybrid form and a on chip continual tunable coplanar delay line. [60] proposes a tunable delay line based on the quadrature directional coupler. Compact wideband antennas suitable for RFID tags are discussed in many recent papers. In [61], a low-cost, wideband planar antenna for RFID tags mountable on metallic surfaces covering 57 MHz bandwidth at a 3-dB return loss has been presented. A wideband antenna for RFID tag that can process 1–2 GHz is also realizable. A UWB antenna operating over 300–2700 MHz with a size less that 15 cm square is reported in [62], while one operating over 400–800 MHz with a size of approximately 10 cm square is reported in [63]. Thus, we believe that suitable antennas are available for use with our proposed RFID tag implementation.

Chapter 4

Design of a covert RFID tag network for target discovery and target information routing

4.1 Introduction

RFID is an exciting area for research due to its relative novelty and exploding growth. Lots of current research on RFID focus on RF tag, reader, communication infrastructure, as well as some policy and security issues [40]. Besides its wide applications in supply chain management, transport, library systems, etc. for object recognition, RFID can also be designed to combine with sensor technologies to support more intelligent applications, such as RFID tag networks for environmental and military monitoring. There are three types of RFID tags: passive tags, semi-passive tags, and active tags. Passive RFID tags use energy from the incoming signal to power themselves, while semi-passive and active RFID tags use internal power source, usually a small battery. Since active RFID tags are battery powered, they have more information storage and processing capabilities, thus they can perform more advanced functionalities compared to traditional passive tags. Besides, they can also work over longer ranges. Active RFID tag is a good candidate for intelligent applications due to its advantages. On the other hand, active RFID tag is subject to failure by battery, which determines that it has limitations, and more factors need to be addressed when using it, such as

i) Its functions should be compatible with the RFIC availability. Very sophisticated algorithms may not be suitable for it.

ii) Its architecture cannot be very complex due to the limited power source. More challenges are in its design, which needs to tradeoff its functionalities and its complexity.

iii) Its communication and data processing section design needs to take account into the RFID tag's architecture complexity.

In this chapter, we explore the application of active RFID tags in target discovery and target information routing in the RFID tag networks, and present the design of a covert RFID tag network for target discovery and target information routing. The scenario is that a static or slowly moving target out of the range of the command center transmits a distinct pseudo-noise signal within the field of the spatially distributed RFID tags, and these RFID tags in the network collect the target's information and route it to the command center. We have the following assumptions:

i) The target is a friendly target, and the noise signal from it is known only to the RFID tags in the network.

ii) The RFID tags in the network do not know their own locations, and the command center has a map of all their locations.

RFID tags in the network detect the target and route the target information to the command center, more data processing tasks are performed at the command center. All the RFID tags in the network are active RFID tags, and can communicate with other RFID tags.

In our design, a noise signal is used as the information carrier to ensure that the communication in the RFID tag network is covert, due to the low probability of interception and low probability of detection of noise waveforms. Noisy tags, which are regular RFID tags that generate noise, can be used to help establish a secure channel between the reader and the queried tag. A noisy tag protocol is proposed in [17], wherein a noisy tag in the reader's field sends out a noise signal generated from a pseudo-random function, the secret shared with the reader. The reader can reconstruct and subtract the noise signals from the noisy tag and recover the message from the queried tag, while an eavesdropper is unable recover the queried tag's message. An eavesdropping-resistant and privacy-friendly RFID system is developed in [64], in which the chip

modulates its reply onto a noisy carrier provided by the reader to protect the back-channel against eavesdropping. This method does not require additional protective devices.

Cluster approaches have been used a lot in parametric frameworks for detection and estimation. Sensors are partitioned into subgroups for distributed learning in the wireless networks [65]. In addition, the cluster approach is also used for topology control [66]. In this chapter, we employ RFID tag clusters within the RFID tag network to collect the target's information. There are two steps in this process: (1) target association, and (2) cluster formation and cluster head selection. If an RFID tag detects the target, then it stores the target's ID and gets associated with the target. Clusters are formed by RFID tags associated with the same target. One of these RFID tags, selected as the head of the RFID tag cluster, routes the target's information out to the command center. In our design, the RFID tag with the maximum number of links to the outside of the cluster is selected as cluster head, which is robust to channel failures, considering that the RFID tags in the network are battery driven and may run out of life. When some of the communication links between the cluster head and those RFID tags out of the cluster are broken, the cluster head RFID tag still can use alternate communication links between it and RFID tags outside of the cluster to route the target's information out.

There are many approaches for information routing in the wireless sensor networks from different aspects of view. In [67], an information-directed routing method is proposed for localization and tracking problems, in which routing is formulated as a joint optimization of data transport and information aggregation, and information accumulated is maximized along the routing path. In [68], selection of the set of cluster heads is defined as the weighted connected dominating set problem, and centralized approximation algorithms are developed to select them. A maximum energy welfare algorithm is designed in [69] by applying the social welfare functions to the routing in wireless sensor networks. Each sensor makes routing decisions to maximize the energy welfare of its local society, which leads to globally efficient energy-

balancing due to overlapping of the local societies. RFID tags can also be used to route information in the networks. In [70], the active relay tags retransmit their received signals during the communication between the interrogator and active tags, and the proposed RFID multi-hop relay system can achieve larger coverage. In our approach, the routing path in the RFID tag network from cluster head RFID tag to the command center is selected according to the channel condition, which is a joint optimization of favorable channel conditions and short path length. Each RFID tag intelligently selects its successor and routes the target's information to it. There are two stages when each node selects its successor on the routing path based on two criteria: (1) channel quality sensing, and (2) target's information routing. During channel quality sensing, the channel condition is estimated and quantized to form the link weight, while in the information routing stage, the RFID tag determines its successor based on the channel information obtained and sends the target's information to it.

In this chapter, we present an algorithm design in the physical layer on target information collection and routing within the RFID tag network in outdoor scenarios, specify the signal format, signal modulation, and signal detection method. Using a noise signal as the information carrier and a noisy key at the front of the RFID tag's signal indicating the purpose of the message, guarantees that the communication within the RFID tag network is covert, owing to the low probability of interception and low probability of detection of the noise waveform. During the RFID tag cluster head selection process, the RFID tag with the maximum number of links to the outside of the cluster is selected as the tag cluster head, and it routes the target information out to the command center. The RFID tag cluster head selected in this manner is robust to channel failures. When some of the communication links between it and the RFID tags out of the cluster turn down, which may occur due to the battery failure in those RFID tags, it still can use the other communication links between it and RFID tags outside of the cluster to route the target's

information out. The routing path from RFID tag cluster head to the command center in the RFID tag network we propose is based on the joint optimization of channel quality and path length.

The rest of the chapter is organized as follows. Section 4.2 gives the design of the RFID tag network and procedures for target's information collection in the RFID tag network. Section 4.3 presents the algorithm for target's information routing within the RFID tag network, and it is illustrated through examples. In Section 4.4, we discuss implementation issues for hardware realization. Section 4.5 draws the conclusions of this chapter and presents possible future extensions.

4.2 Target information collection

In this stage, there are two steps for collecting the target's information: (1) target association, and (2) cluster formation and cluster head selection. In target association, some of the RFID tags detect the target by sensing the environment and record the target's information, and thus these RFID tags are associated with that target. RFID tags associated with the same target form tag clusters. Within a cluster, RFID tags share the same information associated with the target, so when some of the RFID tags turn down due to battery failure, etc., other RFID tags still have the target's information. One RFID tag, namely the head of the RFID tag cluster needs to route the target's information out. The cluster head RFID tag is chosen during cluster head selection.

4.2.1 Target association

The target under monitoring transmits its distinct signal in noise form in the RFID tag field. The RFID tags designed here have templates of the signals from possible targets of interest.

They listen to the environment and detect whether there is any target that is on the monitor list of potential targets. Each RFID tag recognizes the target by comparing its received signal with its template signals in its memory. Once an RFID tag detects a target, it records the target's information, such as the target's ID. Since signal transmitted by the target is of random noise, RFID tags use the cross-correlation process to determine whether the target exists in the field or not. In the real world, the environment is more complex with various interferences such as clutter, Doppler shifts, etc., which are not fully discussed here since they are not the main focus of the chapter.

Suppose the target transmits pseudo-random noise signal burst $s(t)$ over time T_0, and RFID tag has the library of signals from possible targets on the list $\{s_i(t)\}$, $i = 1, 2, \ldots, M$, where M is the number of targets in the monitoring list. That is, in the RFID tag's library, signal $s_i(t)$ is a template of the signal transmitted by the *i*-th target. The detection output at the RFID tag is

$$corr(\tau) = \int_0^T s(t)s_i(t-\tau)dt, \quad for \ j = 1, 2 \ldots, M \tag{4.1}$$

If there is a peak at some time index of the correlation output, it means that the target's signal does exist, and therefore the target's ID is determined.

The RFID tag records the ID of the target that it is associated with to its memory variable $flag_{tag\_id}$, and modulates it to the tag's signal. By default, if an RFID tag is not associated with any target, its $flag_{tag\_id}$ is 0. The RFID tag's signal has the general format as in Figure 4.1, where each section is denoted by the bits under it. For each section, the all-0 bit message means that the RFID tag's signal contains no specific information of that section.

Key	Target ID	Tag ID	Tag ID (o.c.)	Counter
2 bit	2 bit	6 bit	6 bit	3 bit

Figure 4.1. RFID tag's signal general format.

Each RFID tag's base signal comes from filtering a band-limited pseudo-noise signal $s_{tag}(t)$ to a specified and unique frequency sub-band. Different RFID tags have non-overlapping frequency bands, and they all have knowledge of $s_{tag}(t)$ in advance. For example, RFID tag k's base signal $s_{tag\_kb}(t)$ is $s_{tag}(t)$ filtered to its k-th sub-band, and RFID tag k's signal $s_{tag\_k}(t)$ modulated with message is described as

$$s_{tag\_k}(t) = \sum_{n=0}^{L-1} a_n s_{tag\_kb}(t - nT) \tag{4.2}$$

where T is the time duration of $s_{tag\_kb}(t)$, n is the index of the bit, a_n is the valued of the n^{th} bit, and L is the number of total bits of RFID tag's signal.

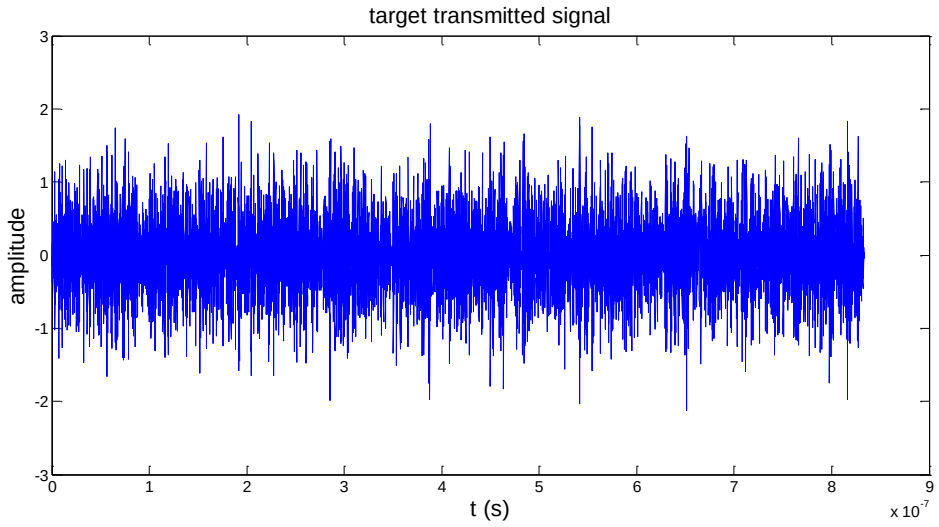
After association with a target, the RFID tag's signal has the format shown in Figure 4.2, where Target ID denotes the target's ID that the RFID tag is associated with.

×	Target ID	Tag ID	×	×

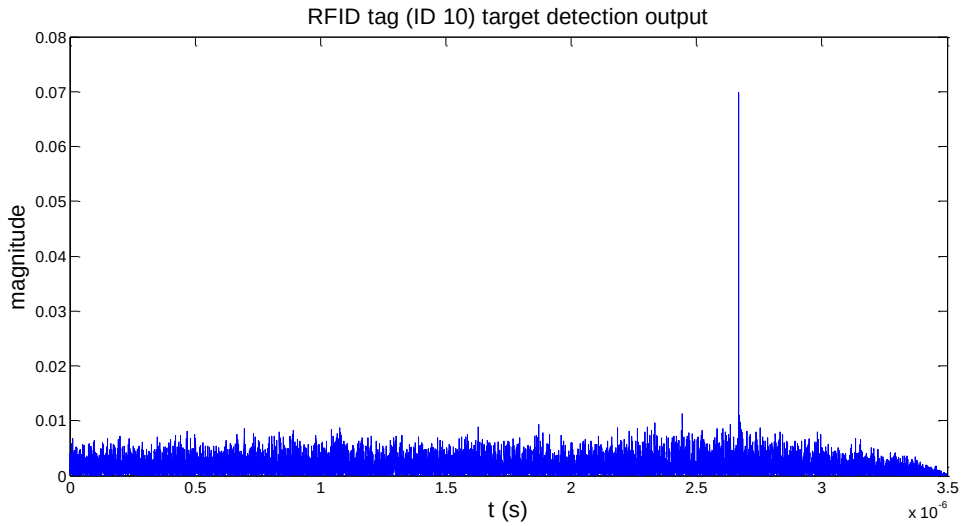
Figure 4.2. RFID tag's signal format after association with a target.

If a target is in the field, only a subset of the RFID tags can collect its information. This is due to the fact that the distance between the target and the RFID tags may be larger than the detection range of some of the tags, or that the channel condition is very bad due to excessive noise making the error probability from that link above the tolerance level.

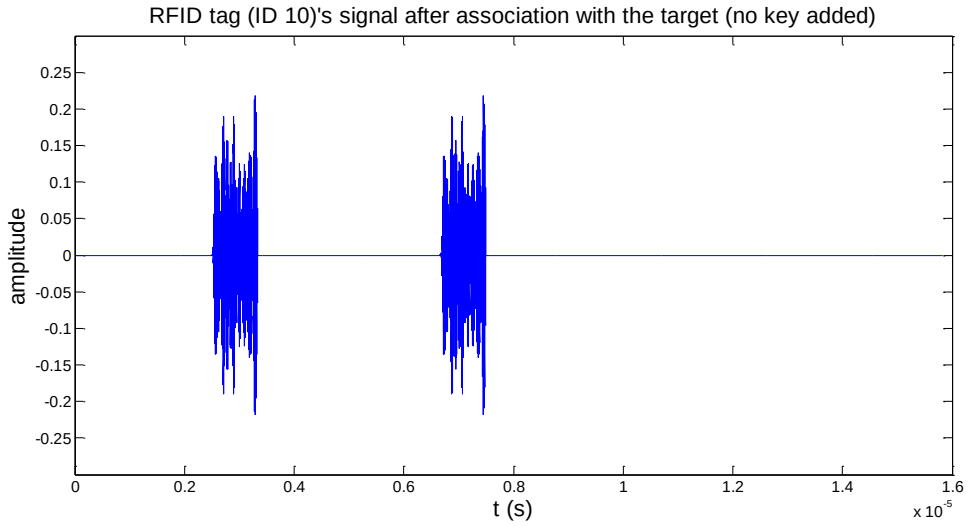
The target association process of an RFID tag is illustrated with simulations in Figure 4.3. In the simulation, the target's signal is assumed to be over the 1-2 GHz frequency band. We also assume that there are 50 RFID tags in the field, the pseudo-noise signal $s_{tag}(t)$ is over 1-2 GHz, and the RFID tag (ID 10)'s signal is over the 1-1.0187 GHz sub-band. RFID tag (ID 10) detects and gets associated with the target (ID 01) in a channel with a signal-to-noise ratio (SNR) of −3 dB. The negative SNR shows that the target association process is performed covertly since the signal power is less than that of the channel noise.



(a)



(b)



(c)

Figure 4.3. Target association simulation illustration. (a) noise signal transmitted by the target; (b) correlation output of RFID tag (ID 10) indicating target detection; (c) RFID tag (ID 10)'s signal after association with a target with no key.

4.2.2 Cluster formation and cluster head selection

RFID tags associated with the same target are formed as a cluster. In each cluster, cluster head RFID tag is selected through inter-communication among the cluster member RFID tags, and is responsible for routing the target's information the cluster's associated with to the outside of the cluster. Using cluster head RFID tag to route the target's information out is to reduce the information redundancy and signal interferences from multiple RFID tags.

RFID tags here are power driven devices, so the links between them may fail occasionally. To ensure connectivity, the RFID tag with the maximum number of links to the outside of the cluster is selected as cluster head, which is responsible for routing the target's information it carries to the outside of the cluster. The cluster head RFID tag selected accordingly is robust to channel failures. When some of the communication links between it and those RFID tags out of the cluster turn down, the cluster head RFID tag still can use the other communication links between it and RFID tags outside of the cluster to route the target's information out.

When a tie occurs, i.e., when two or more concurrent RFID tags have the same number of links to the outside of the cluster, the one with the highest energy level is selected as the cluster head.

We model the RFID tag network as a graph $G(V, E)$, where V is the set of nodes in the graph G, and E is the set of edges. The cluster of RFID tags is modeled as a subgraph C of G. Each RFID tag is represented by a node in the graph and the communication channel between RFID tags is represented by an edge. Then, the cluster head RFID tag is the start node on the routing path of the target's information with which all RFID tags in the cluster are associated.

In our system, the RFID tag is designed to operate in two modes. In Mode I, the default mode, the RFID tag works at normal energy level. In Mode II, the RFID tag works at higher energy and has longer communication distance. Most of the time, the RFID tags operate in Mode

I. In the case an RFID tag needs a larger range, for example, when it tries to find its neighbors but cannot find any in the default mode, the RFID tag will go to Mode II. When the task is finished, the RFID tag will return to the low-energy Mode I.

For the design of the RFID tag's operating Mode II, we assume that each cluster of RFID tags is a connected component in the RFID tag network. That is, for each pair of nodes $u, v \in V(C)$, there is a u, v-path in C. Thus, RFID tags within the same cluster are able to get messages of the rest in the cluster tags. From these messages, the RFID tags recognize other member RFID tags in their cluster and the cluster head RFID tag is determined.

After sensing and association with the target, the RFID tag starts to discover and count its links with RFID tags not associated with the target. The RFID tag associated with the target sends out its outside-link sensing signal of the format shown in Figure 4.4.

Key (1)	Target ID	Tag ID	×	×

Figure 4.4. RFID tag's inquiry signal format for counting outside links.

The Key at the front of the RFID tag's message is globally defined, known by all the RFID tags in the field, to indicate the purpose of the RFID tag's message. Here, Key (1) indicates that the RFID tag which sends out the message is sensing and counting its links with RFID tags outside the cluster. For signal covertness, the Key is designed to be a noise waveform. RFID tags in the network have templates of the Keys, and they can recognize the corresponding Keys by cross-correlating the incoming signal with their stored templates of Keys.

If an RFID tag hears the link inquiry from one RFID tag within the cluster, it obtains the Key in the message and determines the type of the Key. If the Key is Type 1, it decodes the message to get the target's ID. In addition, it checks whether its own signal has that particular

target's ID stored. If it is not associated with the target, it sends back the signal modulated with its ID; else, it does not respond. This guarantees that the RFID tag in the cluster only counts its links with RFID tags outside the cluster. The RFID tag outside the cluster responds to the cluster member RFID tag with the signal format shown in Figure 4.5 upon the link counting inquiry, where Tag ID (o.c.) denotes the RFID tag's ID outside the cluster.

Figure 4.5. RFID tag's response signal format for counting outside links.

The RFID tag stores the number of its links with RFID tags outside the cluster in a counter, which is set to zero (0) by default. RFID tag sensing links with those outside the cluster obtains and determines whether the Key in the message is Type 1 upon its received signal, if so, it decodes the message. It checks whether the first Tag ID in the message is the same as its own to determine whether the message is a response to its link counting inquiry. Then it increases the number of links in its counter by 1 if there is a new RFID tag ID in the message. After searching for links to the outside of the cluster, the RFID tag updates its signal following the format in Figure 4.6, where Counter saves the number of links the RFID tag has to the outside of the cluster, and Key is set to initial value which is blank and has no meaning about the function of the message.

Figure 4.6. RFID tag's signal format after searching for links to the outside of the cluster.

After time Δt_1 from the time it sends out the link counting inquiry signal, the RFID tag stops receiving the responses to its link counting inquiry, and finishes counting the number of links it has with RFID tags outside the cluster. An approximate Δt_1 is given as

$$\Delta t_1 \approx \frac{2R}{c} \tag{4.3}$$

where R is the range of RFID tag, and c is the speed of light in the air.

If the RFID tag cannot find any neighbor outside the cluster at this time, it changes to operation Mode II, and starts searching the links again. In Mode II, the RFID tag functions with more energy than in the default mode. With the design of Mode II, we assume that at least one RFID tag in the cluster has positive Counter. The RFID tag returns to the default operation mode after completing searching its links to the outside of the cluster.

The RFID tags in the cluster that complete the whole searching for links in Mode I wait for time Δt_1 from the time they finish searching for links. Thus, all the RFID tags in the cluster spend the same time $2\Delta t_1$ on the process to search for links to the outside of the cluster.

The link counting process for RFID tag associated with a target is depicted in Figure 4.7.

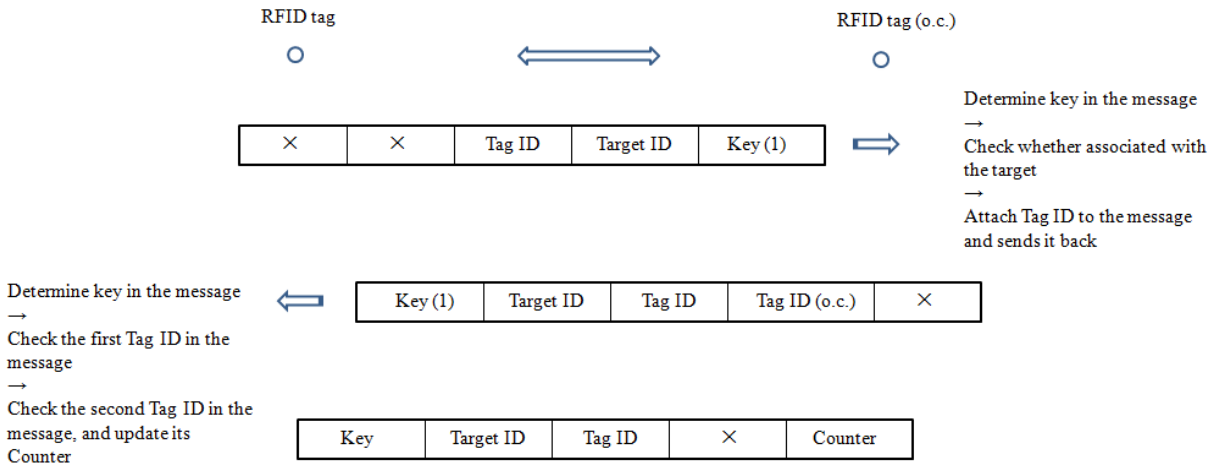


Figure 4.7. Link counting process of RFID tag in the cluster.

Some of the RFID tags in the cluster may be closer to the target than others, so they send out the link count inquiry signals earlier, and complete the link searching and counting process described earlier. We set a time variable $\Delta t_w[tag\_id]$ for each RFID tag to wait after it completes the link searching process, before starting inter-cluster communication. Thus, when the RFID tags in the cluster start inter-cluster communication, they have all finished counting the links and each of their Counters stores the final values.

An approximate value for $\Delta t_w[tag\_id]$ is as follows,

$$\Delta t_w[tag\_id] \approx \frac{K}{t_T[tag\_id]} \tag{4.4}$$

where K is a constant, and $t_T[tag\_id]$ is the target discover time at that RFID tag. Thus, the RFID tag closer to the target wait for longer time after complete searching and counting its links to the outside of the cluster.

Then the RFID tags in the cluster starts inter-cluster communication to recognize the members in the cluster and select the cluster head RFID tag. Each RFID tag broadcasts its signal in the format shown in Figure 4.8, where Key 2 indicates that the message is communicated among RFID tags in the cluster to select the cluster head.

Figure 4.8. RFID tag's format for inter-cluster communication

Upon receiving the signal, the RFID tag in the cluster obtains the Key in the message and determines whether it is Key 2. If it is Key 2, the RFID tags with their $flag_{tag\_id}$ registered will involve in the inter-cluster communication, and those with $flag_{tag\_id}$ of 0 will not. In the case

there is only one target in the field, this also indicates that the RFID tag is within the same cluster. In the complex case of multiple targets in the field, the RFID tag needs to further check the Target ID in the message to determine if it is the same as its own or not. If so, the message is from an RFID tag in the same cluster. After determining that the message is from an RFID tag in the same cluster, the RFID tag continues to decode the message and checks whether the Tag ID in the message is the same as its own. If the message is from another RFID tag for the purpose of cluster head RFID tag selection, it forwards the message and compares the Counter in the message with its own. If the Counter in the message is larger than its own, the RFID tag sets its own Counter to -1, which indicates that its number of links to the outside of the cluster has been compared and not the largest.

After sufficient time Δt_2, each RFID tag in the cluster completes deciding whether it has the most number of links to the outside of the cluster. The RFID tag whose Counter is positive will become the cluster head, and it then starts to route the target's information out. Then all the RFID tags' Counters will be initialized to zero.

An approximation for Δt_2 is given as follows,

$$\Delta t_2 = \frac{2\pi R - R}{c} \ , \tag{4.5}$$

which is a little larger than the worst time of cluster head selection. This approximation for Δt_2 in equation (4.5) is based on the case shown in Figure 4.9.

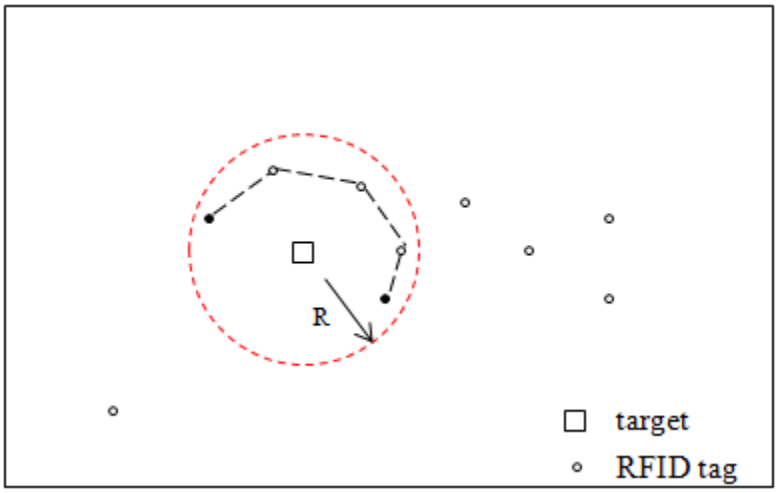


Figure 4.9. Case for maximum Δt_2.

As stated before, the RFID tag network is modeled as a graph, where each node represents an RFID tag and each link represents the communication link between RFID tags. The cluster of RFID tags is then a subgraph, and it is a connected component in our assumption with the design of RFID tag's operation Mode II. In the case shown in Figure 4.9, the two black nodes are in the same cluster, but the distance between them exceeds their range, and they cannot communicate with each other directly. Since the cluster is a connected component, there exists a path in the cluster connecting the two nodes. Through message forwarding by other nodes in the cluster, the two black nodes can communicate indirectly, for example, following the route in dashed line in Figure 4.9. The route length is on the order of $2\pi R - R$, and this costs time on the order of $\frac{2\pi R - R}{c}$. Thus, the cluster head is the RFID tag with the maximum number of links to the outside of the cluster.

In a complex case, several RFID tags in the cluster have the same number of links to the outside of the cluster. Since each RFID tag is ignorant of its location, it does not know whether it is nearest to the command center or not. Thus, the RFID tags in the cluster are unable to select the

one nearest to the command center among them as the cluster head. Instead, they may further communicate to select the one with most energy as the cluster head. In this chapter, we restrict the situation to the simple case that there is no tie.

After a short time, when the target's information is routed to RFID tags that have no links with the RFID tags in the cluster, RFID tags in the cluster set their $flag_{tag\_id}$ to 0, return to the beginning state and start a new cycle. They perform target association, cluster formation, and cluster head selection again.

Additionally, if we upgrade the RFID tag design, as shown in Figure 4.10, such that the cluster head RFID tag is capable of saving the IDs of other RFID tags in the cluster during the inter-cluster communication, and it incorporates that information to the message to be routed outside the cluster, the target's location can also be determined at the command center. As stated before, the command center has a map of all the RFID tags. Thus, if the IDs of at least three RFID tags associated with the target are known, the locations of these three RFID tags are known at the command center, and thereby the location of the target can be determined.

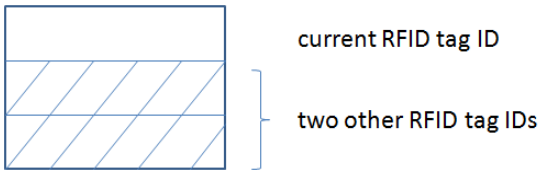


Figure 4.10. Signal format modification for target location determination.

4.3 Target information routing in the RFID tag network

The signal sent by an RFID tag is not of very high power. With the assumption that the communication cost is proportional to the communication distance, the goal of information routing in the RFID tag network is to select a channel which is robust and of short path length to

route the target's information gathered by the RFID tags to the command center. When each node selects its successor on the routing path, there are two stages during the process: channel quality sensing and target's information routing. In channel quality sensing, the link weight is estimated based on the corresponding channel condition. In the information routing stage, the node determines its successor and sends the target's information to it.

The RFID tag network is modeled as a two dimensional graph $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_n\}$ is set of the nodes, representing the RFID tags, and E is the set of bidirectional links, representing the communication links between RFID tags. Each link, shown in Figure 4.11, is assigned a positive weight which indicates the robustness of its corresponding communication channel. If the quality of the communication channel is good, its weight is small; if the channel is bad, for example, very low SNR, excessive fading, object blocked channel, etc., its weight is very large; if there is no link between the two nodes, the weight is ∞. The weight for link (v_i, v_j) is expressed as w_{ij}.

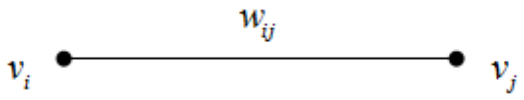


Figure 4.11. Model of a link.

4.3.1 Channel quality sensing

In this step, the RFID tag senses the channels. All its neighbor RFID tags calculate the weights of links connected to them based on their received signals, and respond to the RFID tag with updated messages. If a tag does not find any neighbor, it transmits in power Mode II. The

RFID tag sends out the signal format shown in Figure 4.12 for channel sensing, where Key (3) indicates that the message is for channel sensing.

Counter (/ t(Vi))	×	Tag ID (i)	Target ID	Key (3)

Figure 4.12. RFID tag's signal format for channel sensing.

The channel quality sensing process between two RFID tag nodes is depicted in Figure 4.13. Since RFID tags in the cluster associated with the target have the target ID stored in their memory variables $flag_{tag\_id}$, when they receive the channel quality sensing message indicated by Key (3), they will not respond and thus will not be involved in the target's information routing. As for RFID tags outside the cluster, their memory variables $flag_{tag\_id}$ do not have the target's ID, and they will participate in routing the target's information.

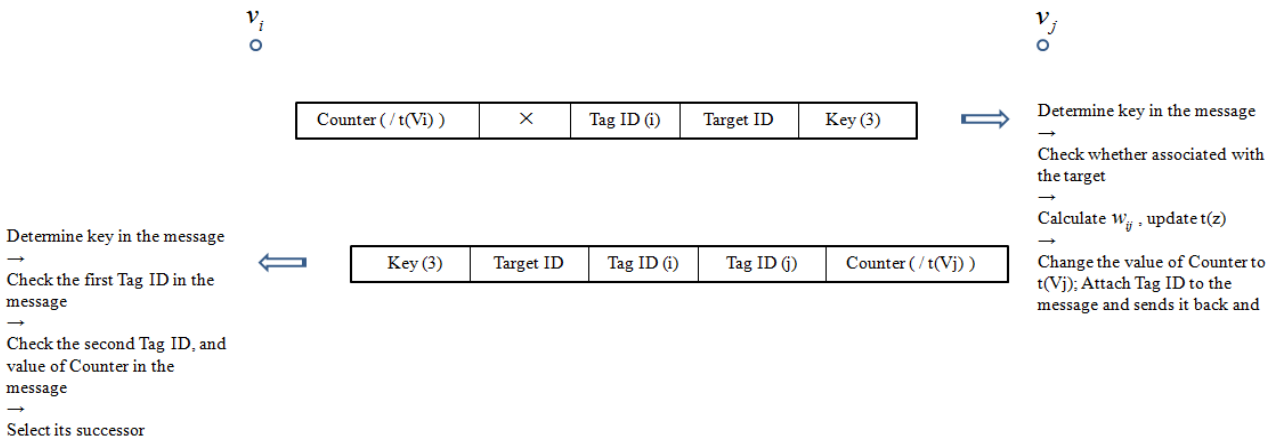


Figure 4.13. Channel quality sensing process between two RFID tag nodes.

In Figure 4.13, node v_j decodes the signal from node v_i, estimates the channel condition for link (v_i, v_j), quantizes it, and grades it to the link weight w_{ij}, generated by a channel quality quantization function. The value of Counter in the message is $t(v_x)$, where $x = i, j$. Also, $t(v)$, $v \in V(G)$ is defined in the information routing section below. The estimation of channel information from the received signal is outside the scope of this chapter. Several papers have discussed this issue, e.g. [71].

The channel condition is quantized and graded to several statuses at the RFID tag, denoted by the weight of the link. The channel quality quantization function may be based on the SNR of the channel, for example, as an inverse function of it. The channel quantization is also not a main concern for discussion in this chapter, and the details are not presented here. Good channel quality is quantized to small link weight, while bad channel quality is quantized to large link weight. An upper limit value $w_{\max}$ for the link weight is established. If the link weight is larger than $w_{\max}$, there is no link between the two nodes or the link between the two nodes is not usable.

4.3.2 Target information routing

The channel aware information routing in the RFID tag network is to find a shortest path with good quality channels from the cluster head RFID tag to the command center.

Since the range of RFID tags is not very large, the length of each hop does not vary much. We model the length of the path as the number of hops from a node to the command center.

Then routing problem then turns into an optimization problem as follows:

$$\min \text{cost} = \left(\sum_{i,j \in \{1,2,..,N\}} w_{ij} x_{ij} + \sum_{i,j \in \{1,2,..,N\}} x_{ij} \right), \quad \text{where } x_{ij} = \begin{cases} 0 \\ 1 \end{cases} \tag{4.6}$$

The first term of the equation denotes the channel condition of each hop. If the channel of the hop is good, then the weight w_i assigned to that link is small. The second term of the equation denotes the length of the path. Thus, equation (4.6) is used to find a routing path with both good link quality and short length.

Equation (4.6) is equivalent to

$$\text{min cost} = \sum_{i,\, j \in \{1,2,\ldots,N\}} w_{ij} x_{ij} \ , \tag{4.7}$$

since the two terms are independent of each other.

Equation (4.7) can be solved using Dijkstra's Algorithm [72]. Given a graph with nonnegative weights and a starting node, Dijkstra's algorithm finds the shortest path from the starting node to other nodes in the graph. Its basic procedure is:

Starting node: u , weights of edges w_{ij}, $i, j \in \{1, 2, \ldots, N\}$

Initialization: $S = \{u\}$, $t(u) = 0$, $t(z) = w_{uz}$ for $z \neq u$

Iteration: Step 1: select a node $v \notin S$ such that $t(v) = \min_{z \notin S} t(z)$; $S = S \cup \{v\}$

Step 2: for each edge vz with $z \notin S$, $t(z) = \min\{t(z), t(v) + w_{vz}\}$

Iteration continues until $S = V(G)$ or $t(z) = \infty$ for each $z \notin S$

Length of shortest path between nodes u, v, is $d(u, v) = t(v)$ for all v.

The stopping rule of the iteration in our algorithm is modified to $v = destination$ or $t(z) = \infty$ for each $z \notin S$.

As for routing through holes, many papers have discussed this issue, such as [73], [74]. Some complete void handling techniques include Greedy Perimeter Stateless Routing (GPSR) [75], Distance Upgrading Algorithm (DUA) [76], etc. We did not expand it here.

We illustrate the operation of the routing path selection algorithm through two examples. Target and cluster member RFID tags are neglected since they are not involved in the information routing process based on the design. The same simulation parameters are assumed as before.

In example 1, 50 nodes are deployed. Each node represents an RFID tag. Node 1 represents the command center, Node 50 represents the cluster head RFID tag, and the blue line represents the link between two nodes. Weight of the link is quantized to 1 or ∞. The topology of example 1 is shown in Figure 4.14.

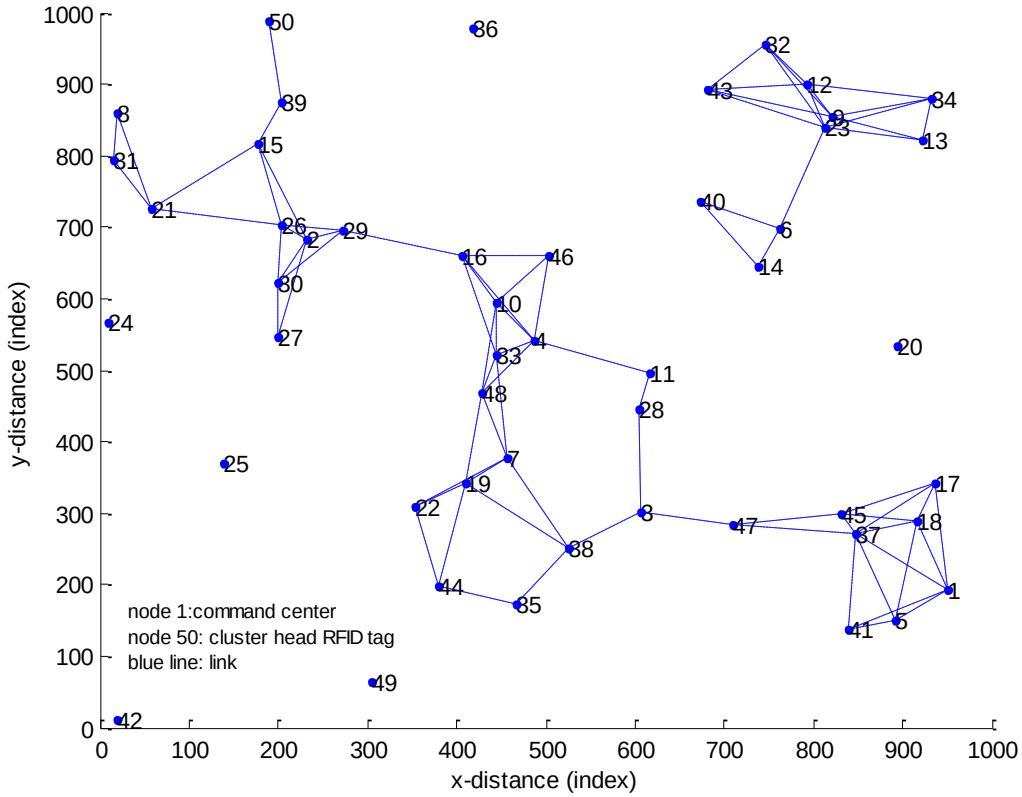


Figure 4.14. Topology of example 1.

Simulation Results:

The target's information routing path from node 50 to node 1 is depicted by the red line in Figure 4.15, which is the shortest path between node 50 and node 1.

Nodes on the routing path are:

path = 50 39 15 2 29 16 4 11 28 3 47 37 1

and the cost of the path, which is the sum of weights of links on the path is:

cost = 12.

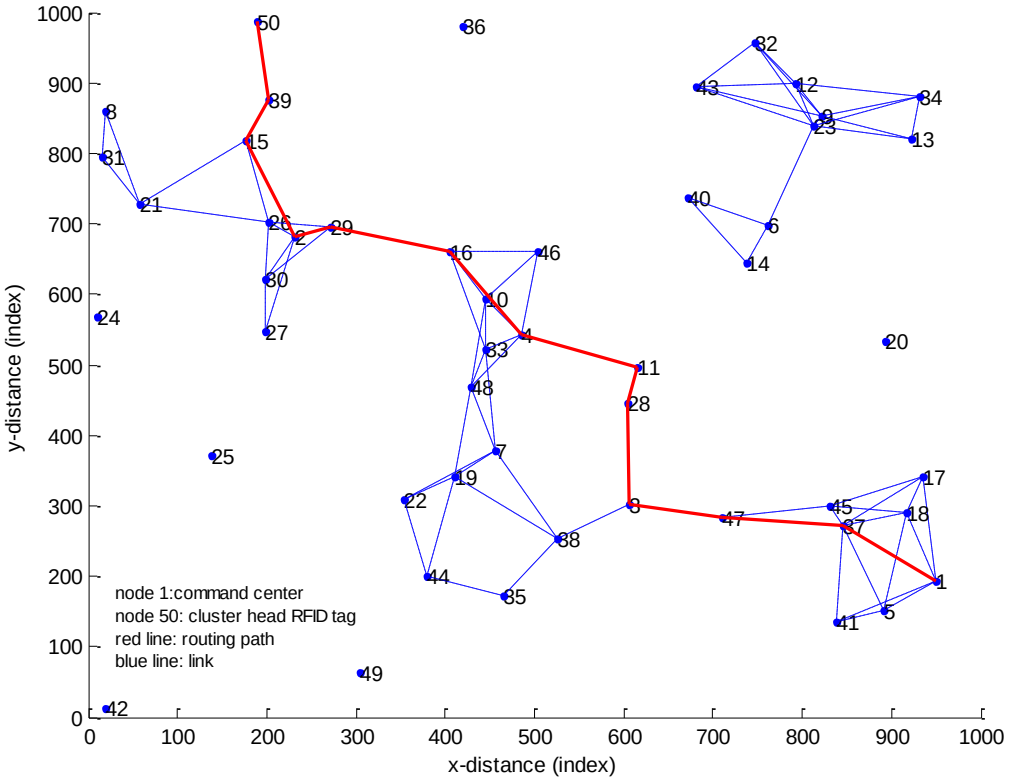


Figure 4.15. Routing path in example 1.

Example 2 is a small network with ten nodes. Weights of the link are quantized to 5, 10, 20, and ∞. The weights of links are described by the matrix W.

$$W = \begin{bmatrix} index & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 0 & 5 & \infty & \infty & \infty & \infty & \infty & 10 & 20 & \infty \\ 2 & 5 & 0 & 5 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\ 3 & \infty & 5 & 0 & 5 & \infty & \infty & 10 & \infty & \infty & \infty \\ 4 & \infty & \infty & 5 & 0 & 10 & \infty & \infty & \infty & \infty & \infty \\ 5 & \infty & \infty & \infty & 10 & 0 & \infty & \infty & \infty & \infty & 10 \\ 6 & \infty & \infty & \infty & \infty & \infty & 0 & \infty & \infty & \infty & \infty \\ 7 & \infty & \infty & 10 & \infty & \infty & \infty & 0 & \infty & 10 & 20 \\ 8 & 10 & \infty & \infty & \infty & \infty & \infty & \infty & 0 & \infty & \infty \\ 9 & 20 & \infty & \infty & \infty & \infty & \infty & 10 & \infty & 0 & \infty \\ 10 & \infty & \infty & \infty & \infty & 10 & \infty & 20 & \infty & \infty & 0 \end{bmatrix} \quad (4.8)$$

Node 1 represents the cluster head RFID tag, and Node 10 represents the command center.

Simulation Results:

The routing path from node 1 to node 10 is:

path = 1 2 3 4 5 10

and the cost of the path is:

cost = 35.

4.4 Hardware implementation considerations

Three important considerations for hardware implementation of the proposed RFID tag structure are: (1) battery life, (2) antennas, and (3) information storage. These are discussed below.

The proposed RFID tags are active RFID tags, meaning that they are designed to both receive commands and transmit coded information to other tags in the vicinity. Because an active RFID tag is powered by the internal energy, the lifetime of the tag is mainly dependent on the lifetime of the battery. However, they have built-in circuitry to turn on the transmitter only when

they receive “wake up” commands. This extends battery life since higher current is drawn only when powering the transmit chain components. In the passive “sleep” mode, these tags act as simple RF receivers which do not require much battery power for functioning. The sleep mode enables the application to shut down the processor of unused modules, thereby saving power [77]. The receiver, which is kept active to react to an inquiry from the interrogator, therefore determines the shelf life of an active RFID tag. To further reduce the power of the RFID tag receiver two main technologies have been proposed: (1) a passive transceiver or burst switch allowing the tag to remain in a sleep mode until activated with RF energy, and (2) a smart buffer, which allows the controller to remain asleep while an incoming packet is buffered [78]. Use of RFID as the wake-up radio channel has been shown to provide a viable solution due to the low cost and ready off-the-shelf availability of RFID [79]. Furthermore, these circuits are able to wake up an entire neighborhood of nodes if a packet at a particular frequency is received.

These RFID tags must necessarily transmit their information in all directions to ensure that the information is assuredly picked up by other randomly distributed tags in the vicinity. This calls for a low-gain omnidirectional antenna, which is quite advantageous since such an antenna comes in smaller packages, and is therefore consistent with the small size of the tag. The antenna must be small enough to be attached to the tag, have omnidirectional or hemispherical coverage must provide maximum possible signal to the receiver, have a polarization matched to the enquiry signal regardless of the physical orientation of the tag, be robust and cheap [80]. Major considerations in antenna selection are antenna type, its impedance, RF performance when applied to the tag and RF performance when the tag has other structures around it. Candidate omnidirectional antennas include the dipole and the folded dipole, with bandwidths of 10-15% and 15-20%, respectively [80]. Planar antennas are low cost, simple to manufacture, and have low profile suitable for RFID systems. The most common types of planar antennas for tags are folded dipoles, meander line antennas (MLAs) and spirals [81]. Planar elliptical patch antennas have

been shown to be adequate for ultrawideband (UWB) applications in several bands. Such UWB antennas have been used in mobile handset devices with FR4 substrate using standard printed circuit board processes. The availability of high-contrast, low-loss ceramic materials permits significant antenna miniaturization, although they have higher loss characteristics [82]. However, their low profile and UWB operation make them quite attractive for use in RFID tags.

Other considerations include storage requirements. The storage size of the RFID tag depends on the number of possible targets to be monitored, size of the target's signal, size of the target ID, size of the tag ID, size of the keys, size of the counter, etc. Since these are application- and scenario- specific, it is difficult to assess the storage requirements in a general sense. It has been proposed that utilizing local storage of writeable RFID tags for inference and query processing makes the distributed approach a better solution with significantly reduced communication cost [83]. The query state primarily dominates the storage cost, and a larger numbers of queries may challenge the scalability of this approach. An approach to exploit the unique property of prime numbers to encode nodes in the path, and simultaneous congruence values to encode ordering between nodes in the path has been implemented and tested in [84]. The encoding scheme is based on the Fundamental Theorem of Arithmetic and the Chinese Remainder Theorem. Using the proposed path encoding scheme, it was shown possible to efficiently retrieve paths which satisfy the path condition in a query [84]. It is assumed in this paper that adequate storage size is available for proper functioning of the tag.

4.5 Conclusions and future work

The design of a covert RFID tag network for target discovery and target's information routing is presented in this chapter. The design and operations of the proposed algorithms are

illustrated through examples. Simulation results clearly demonstrate the effectiveness of the design.

In the design, we also considered the possible physical layer implementations, and considering that RFID tag's structure cannot be made very complex, we make the tradeoffs and do not incorporate too many advanced and accurate functionalities for the RFID tags. Although the initial RFID tag network design goals of the research have been achieved in this chapter, further theoretical and experimental extensions are possible. For the future work, more issues may be investigated to make the design faultless and more practical, such as addressing the holes problem in the RFID tag network during information routing, data traffic and congestion. Implementation of a small RFID tag network based on the design may also be considered.

Chapter 5

Conclusions and Future work

5.1 Conclusions

Radio frequency identification (RFID) tags are small electronic devices working in the radio frequency range. They use wireless radio communications to automatically identify objects or people without the need for line-of-sight or contact. They are widely used in supply chain management, transport, library systems, etc. RFID tags are categorized into three types: passive, semi-passive, and active. Passive RFID tags use energy from the incoming signal to power themselves, while semi-passive and active RFID tags use internal power source, usually a small battery. Active RFID tags have more information storage and processing capabilities, and they can also work over longer ranges. Thus, they can be applied in more intelligent applications compared to traditional passive tags.

This dissertation explores the application of active RFID tags, affixed on friendly assets, operating in outdoor environments and responding to random noise radar interrogations with pre-determined messages. A conceptual system design for communication between the tags and the radar using UWB noise waveforms is proposed and analyzed.

Noise waveform is used to generally maintain covertness and immunity from interference for its randomness feature.

In the proposed design of the system, the RFID tag functional block comprises two parts: the sensing receiver and the active receiver/transmitter considering the efficiency of energy consumption. The sensing receiver is designed to sense the radar header, which is a prearranged secret realization of the noise waveform for the purpose of covertness. The active

receiver/transmitter modulates the RFID tag's message onto the signal through weighted tapped delays considering the simplicity of the RFID tag structure. The RFID tag's ID is embedded through the frequency band of its transmitted signal.

The operation of the system is demonstrated and the performance of the system is analyzed in an AWGN channel. In the example considered for the system design demonstration, where the RFID tag has a 3-tapped delay line, simulation results show that the RFID tags are able to respond to the radar with various kinds of messages. The symbol error probability of the system in the example is at the 10-3 level when the channel SNR is as low as −2 dB, and it still performs well when the channel SNR is −4 dB. Since tag message detection is accomplished via cross-correlation with constantly varying transmit replicas known only to the radar that generates the noise waveform, the radar transmit signal can be maintained smaller and well-concealed within the ambient RF noise.

An algorithm to reduce the interferences caused by multipath signals on the RF tag-to-radar link is presented for the proposed system in the multipath channel case. It is validated through simulations on a test channel.

This dissertation also explores the application of active RFID tags in target discovery and target information routing in the RFID tag networks. The design of a covert RFID tag network for target discovery and target's information routing is presented.

The application scenario is that a static or slowly moving target out of the range of the command center transmits a distinct pseudo-noise signal within the field of the spatially distributed RFID tags, and these RFID tags in the network collect the target's information and route it to the command center. The RFID tags in the network do not know their own locations, and the command center has a map of all their locations.

Noise signal is used as the information carrier and a noisy key is used at the front of the RFID tag's signal indicating the purpose of the message, which guarantees that the

communication within the RFID tag network is covert, owing to the low probability of interception and low probability of detection of the noise waveform.

Target information collection is through two steps: target association, and cluster formation and cluster head selection. Some of the RFID tags detect the target by sensing the environment and record the target's information. Then these RFID tags are associated with the target. RFID tags associated with the same target form a tag cluster. In the cluster, one RFID tag is selected as cluster head, and it is responsible for routing the target's information out of the cluster. That is, the cluster head RFID tag is as the start point of the target information routing path in the network. During the RFID tag cluster head selection process, the RFID tag with the maximum number of links to the outside of the cluster is selected as the tag cluster head. The RFID tag cluster head selected in this manner is robust to channel failures. When some of the communication links between it and the RFID tags out of the cluster turn down, which may occur due to the battery failure in those RFID tags, it still can use the other communication links between it and RFID tags outside of the cluster to route the target's information out.

The routing path in the RFID tag network from cluster head RFID tag to the command center is based on the joint optimization of channel quality and path length. The RFID tag network is modeled as a two dimensional graph, where the nodes represent RFID tags, and the links represent the communication links between RFID tags. Each link is assigned a positive weight indicating the condition of its corresponding communication channel. Small weight means the quality of the channel is good, while large weight means the quality of the channel is bad. When an RFID tag selects its successor, it does the channel quality sensing and estimates and quantizes the channel condition to form the link weight. Then it determines its successor based on the shortest path with good channel quality, and sends the target's information to it.

The design and operations of the proposed algorithms are illustrated through examples. Simulation results demonstrate the effectiveness of the design.

5.2 Future work

Possible future work for the proposed RFID tag system includes the hardware implementation and testing over-the-air. Various mature technologies, e.g., microwave, photonic, and acousto-optic, can be implemented to realize the switchable delay lines at the RF tag for transmitting different messages, as described in [56]–[60]. Compact wideband antennas suitable for RFID tags are discussed in many recent papers. In [61], a low-cost, wideband planar antenna for RFID tags mountable on metallic surfaces covering 57 MHz bandwidth at a 3-dB return loss has been presented. A wideband antenna for RFID tag that can process 1–2 GHz is also realizable. A UWB antenna operating over 300–2700 MHz with a size less than 15 cm square is reported in [62], while one operating over 400–800 MHz with a size of approximately 10 cm square is reported in [63].

Although the initial RFID tag network design goals of the research have been achieved, further theoretical and experimental extensions are possible. For the future work, more issues may be investigated to make the design faultless and more practical, such as addressing the holes problem in the RFID tag network during information routing, data traffic and congestion. Implementation of a small RFID tag network based on the design may also be considered.

Additionally, couplings among nearby RFID tags can be studied. RFID tags are usually made very small in size. Due to its small size, the RF aperture for each RFID tag is not very efficient, and the transmitted power levels are very small. As a result, the detection range is small. When a large number of very small RFID tags are deployed within a small area, there are couplings among the RFID tags. It may be investigated whether there is a way to create a “virtual aperture” by taking advantage of the coupling across RFID tags in close proximity due to the RF field influences. This issue can be approached by analyzing how much the nearby parasitic elements can help improve the pattern of a single active one, which may depends on factors such

as antenna of each element, configuration of the deployment, etc. It can also be studied more explicitly in aspects such as antenna analysis, spatial beamforming, waveform synchronization, and chip and circuit design.

REFERENCES

1. P.G. Ranky, “An introduction to radio frequency identification (RFID) methods and solutions,” Assembly Automation, vol. 26, no. 1, pp. 28–33, 2006.

2. R. Want, “An introduction to RFID technology,” IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, January-March 2006.

3. K.M. Penttila, D.W. Engels, and M.A. Kivikoski, “Radio frequency identification systems in supply chain management,” International Journal of Robotics & Automation, vol. 19, no. 3, pp. 143–151, 2004.

4. L.C. Chen, R.K. Sheu, H.C. Lu, W.T. Lo, and Y.P. Chu, “Object finding system based on RFID technology,” Lecture Notes in Computer Science, vol. 3842, pp. 383–396, 2006.

5. N. Cho, S.J Song, S. Kim, S. Kim, and H.J. Yoo, “A 5.1-μW UHF RFID tag chip integrated with sensors for wireless environmental monitoring,” in Proceedings of the 31st European Solid-State Circuits Conference, Grenoble, France, pp. 279–292, September 2005.

6. S. Saar and V. Thomas, “Toward trash that thinks: product tags for environmental management,” Journal of Industrial Ecology, vol. 6, no. 2, pp. 133–146, February 2008.

7. D.D. Mawhinney, “Microwave tag identification systems,” RCA Review, vol. 44, no. 4, pp. 589–610, December 1983.

8. C.S. Boyd, R.S. Collyer, D.J. Skinner, A.E. Smeaton, S.A. Wilson, D.W. Krause, R.M. Dexter, A.R. Perry, and J. Godfrey, “Characterization of combat identification technologies,” in Proceedings of the IEEE International Region 10 Conference (TENCON 2005), Melbourne, Australia, doi: 10.1109/TENCON.2005.301282, November 2005.

9. R.C. Ormesher, A. Martinez, K.W. Plummer, D. Erlandson, S. Delaware, and D.R. Clark, “Current test results for the Athena radar responsive tag,” in Proceedings of the SPIE Conference on Radar Sensor Technology X, Orlando, FL, vol. 6210, doi: 10.1117/12.664623, May 2006.

10. D.M. Dobkin and T. Wandinger, “A radio-oriented introduction to radio frequency identification,” High Frequency Electronics, vol. 4, no. 6, pp. 46–54, June 2005.

11. H. Stockman, “Communication by means of reflected power,” Proceedings of the. IRE, vol. 36, no. 10, pp. 1196–1204, October 1948.

12. A.R. Koelle, S.W. Depp, and R.W. Freyman, “Short-range radio-telemetry for electronic identification, using modulated RF backscatter,” Proceedings of the IEEE, vol. 63, no. 8, pp. 1260–1261, August 1975.

13. M. Onoe, N. Hasebe, and T. Zamas, “Radar reflectors with controllable reflection,” Electronics and Communications in Japan (Part I: Communications), vol. 63, no. 3, pp. 51–58, March 1980.

14. M. Kossel, H.R. Benedickter, R. Peter, and W. Bächtold, “Microwave backscatter modulation systems,” in IEEE MTT-S Digest, Boston, MA, vol. 3, pp. 1427–1430, June 2000.

15. J.J. Komiak, D.A. Barnum, and D.E. Maron, Digital RF Tag, US Patent no. 7,106,245, issued Sep. 12, 2006.

16. S.D. Blunt and P. Yantham, “Waveform design for radar-embedded communications,” in Proceedings of the International Waveform Diversity and Design Conference, Pisa, Italy, pp. 214–218, June 2007.

17. C. Castelluccia and G. Avoine, “Noisy tags: a pretty good key exchange protocol for RFID tags,” Lecture Notes in Computer Science,, vol. 3928, pp. 289–299, 2006.

18. V. Pillai, R. Martinez, J. Bleichner, K. Elliot, S. Ramamurthy, and K.V.S. Rao, “A technique for simultaneous multiple tag identification,” in Proceedings of the 4th IEEE Workshop on Automatic Identification Advanced Technologies, Buffalo, NY, pp. 35–38, October 2005.

19. D. Puccio, D. Malocha, N. Saldanha, D. Gallagher, and J. Hines, “Orthogonal frequency coding for SAW tagging and sensors,” IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, vol. 53, no. 2, pp. 377–384, 2006.

20. S.D. Blunt, J. Stiles, C. Allen, D. Deavours, and E. Perrins, “Diversity aspects of radar-embedded communications,” in Proceedings of the 2007 International Conference on Electromagnetics in Advanced Applications (ICEAA 2007), Torino, Italy, pp. 439–442, September 2007.

21. M. Roberton and E.R. Brown, “Integrated radar and communications based on chirped spread-spectrum techniques,” in Digest of the 2003 International IEEE Microwave Theory and Techniques Symp. (MTT-S), Philadelphia, PA, pp. 611–614, June 2003.

22. G.N. Saddik, R.S. Singh, and E.R. Brown, “Ultra-wideband multifunctional communications/radar system,” IEEE Transactions on Microwave Theory and Techniques, vol. 55, no. 7, pp. 1431–1437, July 2007.

23. B.H. Cantrell, J.O. Coleman, and G.V. Trunk, Radar Communications. Washington, DC: Naval Research Laboratory (NRL) Report 8515, August 1981.

24. J.L. Burbank, “Enabling the objective force: concepts, technologies, and challenges,” in Proceedings of the 2003 IEEE Military Communications Conference (MILCOM 2003), Boston, MA, pp. 204–208, October 2003.

25. B. M. Horton, “Noise-modulated distance measuring systems,” Proceedings of the IRE, vol. 47, no. 5, pp. 821–828, May 1959.

26. S.E. Craig, W. Fishbein, and O.E. Rittenbach, “Continuous-wave radar with high range resolution and unambiguous velocity determination,” IEEE Transactions on Military Electronics, vol. 6, no. 2, pp. 153–161, April 1962.

27. M. P. Grant, G. R. Cooper, and A. K. Kamal, “A class of noise systems,” Proceedings of the IEEE, vol. 51, no. 7, pp. 1060–1061, July 1963.

28. G. R. Cooper and C. D. McGillem, Random Signal Radar, Final Report TR-EE67-11, Purdue University School of Electrical Engineering, Lafayette, IN, June 1967.

29. J.A. Smit and W.B.S.M. Kneefel, “RUDAR - an experimental noise radar system,” De Ingenieur, vol. 83, no. 32, pp. 99–110, 13 August 1971.

30. J.R. Forrest and J.P. Meeson, “Solid-state microwave noise radar,” Electronics Letters, vol. 12, no. 15, pp. 365–366, 22 July 1976.

31. G. Liu, X. Shi, J. Lu, G. Yang, and Y. Song, “Design of noise FM-CW radar and its implementation,” IEE Proceedings - Part F: Radar and Signal Processing, vol. 138, no. 5, pp. 420–426, October 1991.

32. K.A. Lukin, “Ka-band noise radar,” in Proceedings of the International Symposium on Physics and Engineering of Millimeter and Submillimeter Waves, Kharkov, Ukraine, pp. 322–324, June 1994.

33. R.M. Narayanan, Y. Xu, P.D. Hoffmeyer, and J.O. Curtis, “Design and performance of a polarimetric random noise radar for detection of shallow buried targets,” in Proceedings of the SPIE Conference on Detection Technologies for Mines and Minelike Targets, Orlando, FL, vol. 2496, pp. 20–30, April 1995.

34. E.K. Walton, V. Fillimon, and S. Gunawan, “ISAR imaging using UWB noise radar,” in Proceedings of the 18th Annual AMTA Symposium, Seattle, WA, pp. 167–171, September-October 1996.

35. R.M. Narayanan, Y. Xu, P.D. Hoffmeyer, and J.O. Curtis, “Design, performance, and applications of a coherent ultrawideband random noise radar,” Optical Engineering, vol. 37, no. 6, pp. 1855–1869, June 1998.

36. I.P. Theron, E.K. Walton, S. Gunawan, and L. Cai, “Ultrawide-band noise radar in the VHF/UHF band,” IEEE Transactions on Antennas and Propagation, vol. 47, no. 6, pp. 1080–1084, June 1999.

37. R. Stephan and H. Loele, “Theoretical and practical characterization of a broadband random noise radar,” IEEE MTT-S International Microwave Symposium Digest, Boston, MA, pp. 1555–1558, June 2000.

38. L. Turner, “The evolution of featureless waveforms for LPI communications,” in Proceedings of the IEEE 1991 National Aerospace and Electronics Conference (NAECON), Dayton, OH, pp. 1325–1331, May 1991.

39. S.R.J. Axelsson, “Random noise radar/sodar with ultrawideband waveforms,” IEEE Transactions on Geoscience and Remote Sensing, vol. 45, no. 5, pp.1099–1114, May 2007.

40. Ngai, E.W.T.; Moon, K.L.; Riggins, F.J.; Yi, C.Y. “RFID research: An academic literature review (1995–2005) and future research directions”. Int. J. Prod. Econ., 2008, 112, 510-520.

41. P. Bidigare and M. Nayeri, “RF tags: radar as a communications channel,” in Proceedings of the 10th Adaptive Sensor Array Processing (ASAP) Workshop, Lexington, MA, http://www.ll.mit.edu/asap/asap_02/Proceedings/Presentations/Bidigare.pdf, March 2002.

42. P. Bidigare, “The Shannon channel capacity of a radar system,” in Record of the Thirty-Sixth Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, pp. 113–117, November 2002.

43. Dong-Liang Wu, Wing W.Y.NG, Daniel S. Yeung, Hai-Lan Ding, “A brief survey on current RFID applications”, Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009.

44. Deva Seetharam, Richard Fletcher, “Active tag zoo”, www.rfidjournal.com/whitepapers/10/2.

45. Se-gon Roh, Hyouk Ryeol Choi, “3-D tag-based RFID system for recognition of object”, IEEE Transactions on Automation Science and Engineering, vol. 6, no. 1, pp. 55-65, 2009.

46. Gaetano Marrocco, “Self-sensing passive RFID tags”, http://www.ursi.org/proceedings/procGA08/papers/D01p7.pdf.

47. Bill Glover, Himanshu Bhatt, RFID Essentials, O’ Reilly Media, Inc. 2006.

48. J.G. Proakis, Digital Communications (4th ed.). New York, NY: McGraw-Hill, 2001.

49. L.A. Aroian, “The probability function of the product of two normally distributed variables,” Annals of Mathematical Statistics, vol. 18, no. 2, pp. 265–271, June 1947.

50. Q. Tianshu, W. Shuxun, C. Haihua, and D. Yisong, “Adaptive denoising based on wavelet thresholding method,” in Proceedings of the 6th International Conference on Signal Processing (ICSP’02), Beijing, China, pp. 120–123, August 2002.

51. M. Nakhkash and A. Mirzaei, “Wavelet denoising applied to free-space reflection measurements,” Measurement Science and Technology, vol. 19, no. 11, doi: 10.1088/0957-0233/19/11/115706, November 2008.

52. R.Q. Quiroga and H. Garcia, “Single-trial event-related potentials with wavelet denoising,” Clinical Neurophysiology, vol. 114, no. 2, pp. 376–390, February 2003.

53. D.L. Donoho, “De-noising by soft-thresholding,” IEEE Transactions on Information Theory, vol. 41, no. 3, pp. 613–627, May 1995.

54. W. Zhang and X.H. Zhao, “Wavelet thresholding using higher-order statistics for signal denoising,” in Proceedings of the 2001 International Conference on Info-Tech and Info-Net (ICII 2001), Beijing, China, vol. 1, pp. 363–368, October-November 2001.

55. A. Jensen and A. la Cour-Harbo, Ripples in Mathematics—The Discrete Wavelet Transform, Springer, Berlin (2001).

56. E.N. Toughlian and H. Zmuda, "A photonic variable RF delay line for phased array antennas," IEEE Journal of Lightwave Technology, vol. 8, no. 12, pp. 1824–1828, December 1990.

57. T.C. Cheston, H.P. Coleman, and J.B.L. Rao, Ultrawideband Scanner Array Architecture. Washington, DC: Naval Research Laboratory (NRL) Report MR/5310, June 1995.

58. R.Y. Loo, G.L. Tangonan, H.W. Yen, J.J. Lee, V.L. Jones, and J. Lewis, "5 bit photonic time shifter for wideband arrays," Electronics Letters, vol. 31, no. 18, pp. 1532–1533, 31 August 1995.

59. P. Abele, R. Stephan, M. Birk, D. Behammer, H. Kibbel, A. Trasser, K.B. Schad, E. Sonmez, and H. Schumacher, "An electrically tunable true-time-delay line on Si for a broadband noise radar," in Digest of the 2003 Topical Meeting on Silicon Monolithic Integrated Circuits in RF Systems, Garmisch, Germany, pp. 130–133, April 2003.

60. A.A. Pohvalin and S.V. Krasilnikov, "Tunable delay line on quadrature bridge with digitally controlled group delay characteristic," in Proceedings of the 15th International Crimean Conference on Microwave & Telecommunication Technology (CriMiCo 2005), Sevastapol, Ukraine, pp. 593–594, September 2005.

61. L.W. Son, J. Yeo, G.Y. Choi, and C.S. Pyo, "A low-cost, wideband antenna for passive RFID tags mountable on metallic surfaces," in Proceedings of the 2006 IEEE Antennas and Propagation International Symposium, Albuquerque, NM, pp. 1019–1022, July 2006.

62. J.C. Adams, W. Gregorwich, L. Capots, and D. Liccardo, "Ultra-wideband for navigation and communications," Proceedings of the 2001 IEEE Aerospace Conference, Big Sky, MT, pp. 2/785–2/792, March 2001.

63. Y.J. Ren, C.P. Lai, P.H. Chen, and R. M. Narayanan, "Compact ultrawideband UHF array antenna for through-wall radar applications," IEEE Antennas and Wireless Propagation Letters, vol.8, pp. 1302–1305, 2009.

64. Hancke, G. Modulating a noisy carrier signal for eavesdropping-resistant HF RFID. Elektrotechnik und Informationstechnik, 2007, 124, 404-408.

65. Predd, J.B.; Kulkarni, S.R.; Poor, H.V. Distributed learning in wireless sensor networks. In Wireless Sensor Networks: Signal Processing and Communications Perspectives; Swami, A., Zhao, Q., Hong, Y.-W., Tong, L., Eds. John Wiley & Sons: Chichester, UK, 2007; pp. 185-214.

66. Chu, K.-T.; Wen, C.-Y.; Ouyang, Y.-C.; Sethares, W.A. Adaptive distributed topology control for wireless ad-hoc sensor networks. In Proceedings of 2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), Valencia, Spain, 14–20 October 2007; pp. 378-386.

67. Liu, J.; Zhao, F.; Petrovic, D. Information-directed routing in ad hoc sensor networks. IEEE J. Sel. Area. Comm., 2005, 23, 851-861.

68. Zhang, C. Cluster-based routing algorithms using spatial data correlation for wireless sensor networks. J. Communications, 2010, 5, 232-238.

69. Ok, C; Lee, S.; Mitra, P.; Kumara, S. Distributed routing in wireless sensor networks using energy welfare metric. Inform. Sciences, 2010, 180, 1656-1670.

70. Hong, S.H; Zhang, H.; Song, I.C.; Chang, K.H.; Shin, D.-B. ; Lee, H.-S. ISO/IEC 18000-7 based on RFID multi-hop relay system. In Proceedings of the 9th International Symposium on Communications and Information Technology (ISCIT 2009), Incheon, Korea, 28–30 September 2009; pp. 1450-1454.

71. Wada, T.; Jamalipour, A.; Okada, H.; Ohuchi, K.; Saito, M. Performance of channel information estimation method utilizing parity check bits for Turbo coded multi-route multi-hop networks. In Proceedings of the 2006 IEEE International Conference on Communications (ICC'06), Istanbul, Turkey, 11–15 June 2006; pp. 3688-3692.

72. West, D.B. Introduction to Graph Theory, 2nd ed. Prentice Hall: Upper Saddle River, NJ, USA, 2001; pp. 97-98.

73. Ahmed, N.; Kanhere, S.S.; Jha, S. The holes problem in wireless sensor networks: A survey. SIGMOBILE Mobile Computing and Communications Review, 2005, 9, 4-18.

74. Joshi, G.P.; Kim, S.W. A distributed geo-routing algorithm for wireless sensor networks. Sensors, 2009, 9, 4083-4103.

75. Hightower, J.; Borriello, G. Location system for ubiquitous computing. Computer, 2001, 34, 57-66.

76. Chen, S.; Fan, G.; Cui, J.-H. Avoid 'void' in geographic routing for data aggregation in sensor networks. Int. J. Ad Hoc Ubiq. Co., 2006, 1, 169-178.

77. Cho, H.; Baek, Y. Design and implementation of an active RFID system platform. In Proceedings of the International Symposium on Applications and the Internet Workshops (SAINTW'06), Phoeniz, AZ, USA, 23–27 January 2006; doi: 10.1109/SAINT-W.2006.14.

78. Jones, A.K.; Hoare, R.R.; Dontharaju, S.R.; Tung, S.; Sprang, R.; Fazekas, J.; Cain, J.T.; Mickle, M.H. An automated, reconfigurable, low-power RFID tag. In Proceedings of the 43rd Annual Design Automation Conference (DAC'06), San Francisco, CA, USA, 24–28 July 2006; pp. 131-136.

79. Jurdak, R.; Ruzzelli, A.G.; O'Hare, G.M.P. Multi-hop RFID wake-up radio: Design, evaluation and energy tradeoffs. In Proceedings of 17th International Conference on Computer Communications and Networks (ICCCN '08), St. Thomas, US Virgin Islands, USA, 3–7 August 2008; doi: 10.1109/ICCCN.2008.ECP.124.

80. Foster, P.R.; Burberry, R.A. Antenna problems in RFID systems. In Proceedings of the IEE Colloquium on RFID Technology, London, UK, 25 October 1999; pp. 3/1-3/5.

81. Serrano, R.; Blanch, S.; Jofre, L. Small antenna fundamentals and technologies: Future trends. In Proceedings of the First European Conference on Antennas and Propagation (EuCAP 2006), Nice, France, 6–10 November 2006; doi: 10.1109/EUCAP.2006.4584659.

82. Ren, Y.-J.; Lai, C.-P.; Chen, P.-H.; Narayanan, R.M. Compact ultrawideband UHF array antenna for through-wall radar applications. IEEE Antennas Wireless Propag. Lett., 2009, 8, 1302-1305.

83. Cao, Z.; Diao, Y.; Shenoy, P. Architectural considerations for distributed RFID tracking and monitoring. In Proceedings of the ACM Workshop on Networking Meets Databases (NetDB), Big Sky, MT, USA, 14 October 2009.

84. Lee, C.-H; Chung, C.-W. Efficient storage scheme and query processing for supply chain management using RFID. In Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data (SIGMOD'08), Vancouver, BC, Canada, 9–12 June 2008; pp. 291-302.

VITA

Qihe Pan

Education

2006.8 – 2011.12 **Ph.D.** in Electrical Engineering, The Pennsylvania State University

2002.9 – 2006.7 **B.E.** in Electronic Engineering, Tsinghua University, China

Publications

Qihe Pan and R.M. Narayanan, "Delay modulated RF tag system concept using ultrawideband noise radar waveforms," accepted in *International Journal of Distributed Sensor Networks*, 2011.

Qihe Pan and R.M. Narayanan, "Design of a covert RFID tag network for target discovery and target information routing," accepted in *Sensors Journal*, 2011.

Qihe Pan and R.M. Narayanan, "An RF tag communication system model for noise radar," Proc. SPIE Conference on Wireless Sensing and Processing III, Orlando, FL, vol. 6980, pp. 698007-1–698007-12, doi:10.1117/12.777394, March 2008.