A Secure Wireless Network for Roadside Surveillance using Radio Tomographic Imaging

Robert Paul S. Inglis, Ryan P. Brenner, Erin L. Puzo, T. Owens Walker III, Christopher R. Anderson
Department of Electrical and Computer Engineering
United States Naval Academy, Annapolis, MD
{ofc23258, owalker, canderso}@usna.edu

Ryan W. Thomas, Richard K. Martin
Department of Electrical and Computer Engineering
Air Force Inst. Of Technology, Wright-Patterson AFB, OH
richard.martin@afit.edu

Abstract—This paper proposes and demonstrates the novel application of a secure wireless sensor network for roadside surveillance and vehicular detection using radio tomographic imaging. Network architecture is based on the well-established Zigbee standard and medium access is provided through a time division multiple access scheme. Wireless security vulnerabilities are considered and a four-part security scheme is presented. Field test results are provided to validate both the baseline radio tomographic imaging functionality and the accompanying wireless sensor network security mechanisms.

Keywords—wireless sensor network (WSN), wireless security, radio tomographic imaging (RTI), network tomography, jamming mitigation, node authentication, transmission encryption

I. INTRODUCTION

Wireless Sensor Networks (WSNs) offer the potential to increase data collection or processing capabilities across a broad range of applications for a minimal investment of manpower. A WSN typically consists of some number of wireless sensor nodes each comprised of a power supply, a processor, a radio transceiver, and a suite of application-dependent sensors. WSNs are frequently employed to implement a “smart environment” or to gather data over a given area [1]. Examples of such networks include fully interactive home electronics systems [2] and meteorological survey WSNs used monitor simple weather indicators over a region [3] as well as military applications such as remote battlefield monitoring [4] and signals collection [5].

This work proposes the novel application of wireless sensor network radio tomographic imaging (RTI) to provide secure remote roadside surveillance. This wireless sensor network provides the capability to securely and autonomously monitor vehicular traffic along roadways by detecting and identifying passing vehicles using radio tomographic imaging. With application to both the military and civilian sectors, it can provide remote surveillance of enemy combatant movement as well as monitoring and management of traffic flow on major commuter arteries.

The main contributions of this work are (1) the novel design and implementation of a roadside surveillance WSN using RTI to detect and identify vehicular traffic and (2) the design and implementation of an accompanying wireless security system. Design constraints are considered and field results are provided to demonstrate the effectiveness of the proposed network. To the best of our knowledge, this is the first implementation and successful field test of a secure wireless sensor network roadside surveillance application using radio tomographic imaging.

This paper is organized as follows. Background discussions in the areas of Radio Tomographic Imaging and WSN security are provided in Section II. The design and operation of the RTI-capable WSN is presented in Section III and the accompanying security scheme is proposed in Section IV. The results from two field tests are provided in Section V.

II. BACKGROUND

In this section, we present a summary of the important points related to Radio Tomographic Imaging and Wireless Sensor Networks security.

A. Radio Tomographic Imaging

While many techniques exist for roadside surveillance and the accompanying localization and tracking functions, there are a number of significant drawbacks in the existing proposals. Image-based positioning requires a camera to have an unobstructed view of the object and good illumination conditions [6]. RF direction-finding techniques require the object to have an active transmitter and multiple receivers that cannot be subject to jamming or interference [7], [8], [9]. GPS requires a clear, unobstructed view of the sky and the ability to track multiple satellites, conditions which can easily be degraded in forest or indoor environments [10].

Radio tomographic imaging (RTI), developed by Wilson and Patwari [11], provides a means for localizing and tracking the position of an object inside a sensor network. RTI operates by using a wireless sensor network in a fully-interconnected mesh configuration where each node monitors the received signal strength from every other node. As objects move into the network, they will physically obstruct one or more links. Links that are obstructed will experience losses due to reflection, diffraction, and object attenuation. As a result, the received signal strength (RSS) on those links will decrease relative to a pre-calibrated or previously measured baseline free space value. By monitoring which links are attenuated and by how much, it is possible to determine the position, size, and mass of the object in the network [12]. Additionally, objects that are actively broadcasting a jamming signal may still be roughly located simply by monitoring which links have been jammed.
By evaluating links that are being jammed and those that are not, the network is able to determine the approximate source of the jam field and track the object [13].

B. WSN Security

As WSNs are deployed more commonly and deal increasingly with sensitive, private, or mission-critical information, the need for WSN security grows correspondingly. The development of WSN security is influenced by the distinguishing traits of WSNs: limited processing capabilities, a finite power supply, and deployment in remote locations to function autonomously. Thus, the security concerns relevant to WSNs differ from those of traditional wireless networks.

Threats to WSNs can be divided into external and internal attacks. External attacks can be further sub-categorized as passive attacks, which typically consist of unauthorized listening, or external attacks, which usually take the form of a denial of service attack involving some variety of jamming or power exhaustion. Internal attacks consist of the infiltration of the WSN by a foreign node, or the corruption and compromise of an existing sensor node within the network [14].

Potential attacks on WSNs include jamming, tampering, intended collision, energy-exhaustion, flooding, node desynchronization, and spoofed, altered, or replayed routing information. Areas of concern in WSN security can be summarized as cryptography, key management, attack detection and prevention, secure routing, secure location, secure data aggregation, security-energy assessment, data assurance, and survivability [14].

III. SENSOR NETWORK DESIGN

We now describe the wireless sensor network used in this work and the layout of its nodes. Additionally, we provide a description of networked RTI operation.

A. Sensor Platform

The RTI sensor network is comprised of a number of wireless sensor nodes and one aggregate control node. The hardware of every node is fundamentally the same. The command and control (C2C) node, though, is programmed with different software code. A schematic of the circuit board used is shown in Figure 1. This circuit board features a battery power source, microprocessor, and XBee ZigBee Pro RF module, as shown in Figure 2. Nodes use the DSPIC33FJGP302 microprocessor, which is configured to interface with the XBee module. In transmissions, the XBee is set to use Advanced Peripheral Interface (API) mode to ensure easily recognizable packet formats.

B. Operation

The network collects data by measuring the RSS of packets sent between nodes. Nodes transmit sequentially in a Time Division Medium Access (TDMA) scheme initiated by a start packet broadcast by the C2C node, which synchronizes all the sensor nodes. A single scan of the network begins with this start packet, and each sensor node is allocated one time slot in the scan. Within its respective time slot, each node broadcasts a packet to the network that includes both its identity (node number) and the most recent RSS values it has recorded from the prior scan (one for each other node in the network). The remaining nodes in the network listen for this transmission, and measure and record the RSS value of the packet received. Figure 4 illustrates one such transmission taking place. At the completion of the scan, each node will have knowledge of the most recent signal strength between itself and every other node in the network array.

During each scan, the C2C node will send the start packet and then listen to the nodes’ transmissions for the remainder of the scan time. Because each node broadcasts its data packet to the entire network, an additional listening node configured for monitoring purposes is able to receive and record the RSS information in real time. This node is an XBee RF Module, connected to a PC via RS232, which is able to observe and record all RSS information using a capture text program. The resulting data can be used to piece together a three dimensional picture of any impeding object in the area within the network [11].

One limitation of the network is the speed at which it can detect objects moving through the network. This speed is limited by the length of time it takes to perform a single scan of the network area. In turn, the scan time is ultimately determined by the XBee data rate and amount of information sent in each packet. For a linear network configuration, such as...
one that might be used to monitor vehicle traffic along a road [13],[15], it is critical to be capable of accurately tracking vehicles moving at typical highway speeds. Figure 3 illustrates the format of the data packet used in our network, which is typical of the packet format used in a RTI WSN system.

The time required for one scan of the network is given by

\[
\tau_{scan} \geq \left( \frac{k_{bits}}{n_{rate}} \right)
\]  

(1)

where \(k_{bits}\) is the total number of bits which need to be transmitted in a single scan, \(n_{rate}\) is the rate at which data is transmitted in bits/second, and \(\tau_{scan}\) is the amount of time in seconds required for a full scan of the network to occur. To account for the time needed by a node to process each packet, the value \((k_{bits} / n_{rate})\) represents a lower bound for \(\tau_{scan}\). In a linear configuration, the minimum desired object resolution will be inversely proportional to the maximum speed of the vehicle, as given by

\[
\frac{r_{dist}}{\tau_{scan}} = v_{det}
\]

(2)

where \(r_{dist}\) is the voxel size, and \(v_{det}\) is the maximum movement velocity in meters/second at which objects moving through the network can be detected. The area scanned by the network is divided into some number of voxels. The voxel length is related to the resolution of images produced from the network’s RSI data, and represents the desired minimum resolution in meters for detecting objects. This value influences the velocity at which objects moving through the network can be determined, since an object cannot be detected if it exits a given voxel before a single scan can be completed.

The network implementation presented in this work was designed as a sample proof of concept and uses the following specifications: \(s_{det} = 10\ mph = 4.704\ m/s\), \(r_{dist} = 0.75\ m\), \(n_{rate} = 9600\ bps\).

IV. SECURITY

As discussed in Section II, a number of security vulnerabilities exist in the baseline WSN that need to be addressed to ensure robust operation. For example, the unsecured RTI wireless sensor network design is vulnerable to RF jamming attacks, covert node replacement, false data transmission, and transmission tapping by unintended listeners. In this section we discuss the design and implementation of security solutions to these vulnerabilities.

The security scheme presented here consists of four components, listed below. A functional decomposition is also shown in Figure 5.

1. **Message Encryption**: The network implements an encryption protocol to ensure secure and private transmission of network traffic.

2. **Jamming Mitigation**: The network is configured to minimize the effects of jamming (i.e. malicious noise or interference in the transmission channel) on network operation.

3. **Network Topology**: The control node is able to detect the presence of nodes dropping off of and rejoining the network.

4. **Node Authentication**: If a new node joins the network, the control node initiates a ‘Challenge-and-Response’ confirmation to ensure that the node is authorized to be on the network.

This list of security features is not exhaustive since we have limited our work to a subset of commonly targeted security vulnerabilities. These specific vulnerabilities were chosen because they address the fundamentals of network security [16]. A good example of potential follow-on work is the network’s ability to withstand energy depletion attacks.

<table>
<thead>
<tr>
<th>Overhead</th>
<th>I.D. #</th>
<th>RSS Packet Data</th>
<th>Sensor Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 Bytes</td>
<td>2 Char</td>
<td># Nodes x 1 Char (2 Bytes)</td>
<td># Nodes x 1 Char (2 Bytes)</td>
</tr>
</tbody>
</table>

Figure 3. Illustrates an example data packet within our WSN.

Figure 4. Illustration of first node broadcasting in the TDMA scheme. Image from [15]
A. Jamming Mitigation

To provide Jamming Mitigation and minimize the effects of outside noise and interference, we make use of a frequency hopping scheme. This design utilizes a frequency hopping scheme in which the network cycles through a series of different frequencies without regard to whether a jamming signal is present. This is a proactive approach and a significant benefit to this design is that the overhead associated with identifying the presence of interference can be eliminated. It comes at the expense of a slight increase in scan time and code complexity. An alternative design utilizing a reactive system would periodically measure the channel for interference or jamming signals and would only initiate frequency hopping when such a signal was found. Although the reactive system provides a lower overhead cost to network operation in terms of channel switching when channel noise is not significant, the task of adaptively coordinating the XBee nodes on a new channel after each hop in an order and frequency determined during runtime adds significant complexity to the scheme.

The XBee RF Modules incorporate 16 selectable RF channels across which chips are preconfigured to transmit. Channel frequencies are described by the equation

\[ f_c = 2.405 \text{GHz} + (CH - 11) \times 5 \text{MHz} \]  

(3)

where \( f_c \) is center frequency, and \( CH \) represents the channel number (ranging from 0x0C to 0x17). Channel assignments are non-overlapping. In other words, XBee modules operating on different frequencies are not able to communicate and their transmissions do not interfere with each other [17]. In our implementation, all nodes switch transmitting frequency simultaneously, according to a prearranged hop table. In practice, the hopping sequence can also be generated through the use of a pseudo-random sequence known only to the authorized nodes [18].

B. Transmission Encryption

To protect the privacy of the information exchanged during WSN operation, we implemented a Transmission Encryption scheme designed to encrypt network data packets.

The XBee RF Modules include support for an AES (Advanced Encryption Standard) 128-bit symmetric key. This solution was selected because it meets the functional requirements of this work and can be directly implemented in any XBee-based network. This decreases network throughput though, as each data packet must append an additional 16 bytes of overhead and each message encryption or decryption adds a slight processing delay. In our network, the additional overhead increased the average packet length by roughly 50%, though this result will vary for different network designs.

To secure the network from unauthorized outside surveillance, all nodes operating on the network are encoded using a single main KY (encryption key) value which acts as the symmetric key for encrypted network traffic. To avoid key management issues (which are beyond the intended scope of this work), we chose to limit the keys used to a pre-distributed set. All nodes are set to Encryption Enabled (EE) mode and loaded with the predetermined KY values. Nodes are programmed to have their EE and KY parameters set during the initialization phase of node start-up. API formatted AT commands are sent from the dsPIC to the XBee module to enable encryption during runtime and they follow the packet structure shown in Figure 6. These parameters need not be reset except in select circumstances (as outlined below in Section D).

C. Network Topology

The goal of the network topology portion of our security scheme is to track the addition and loss of nodes entering and exiting the network. For this application, the network is designed to run using a fully connected mesh network topology with a central controller and is not intended to support ad-hoc capabilities.

The diagram in Figure 7 outlines the state machine logic that determines how the control node tracks sensor nodes during the RSS transmit loop. A node will be ‘dropped’ from the network if it consecutively misses (i.e. does not transmit during) some set number of network scans. The control node observes the network across each scan cycle and records which nodes do not respond within their assigned time slot according to the TDMA scheme. The control node maintains a counter for each sensor node within the network. Each counter increments whenever the associated node successfully transmits, up to some predetermined maximum, and decrements whenever a node fails to do so, down to a minimum value of zero. If a node’s counter reaches a value of zero, it is dropped from the network and is marked accordingly by the control node. If a

![Diagram showing packet structure for Encryption Enable AT Command (ATEE) on the XBee module.](image)

![Diagram showing state machine logic for Node Topology tracker in control mode.](image)
node begins retransmitting after some absence, the control node recognizes that node as a new, unauthenticated node seeking to join the network and implements a Node Authentication check, as described in Section D, before recognizing the node as trusted once more.

The underlying RTI network design influences how we approach this problem. Due to the TDMA scheme utilized, unauthorized nodes attempting to fully infiltrate the network will need to occupy a time slot previously vacated by an authorized node which has dropped off the network. Thus, the network topology scheme is intended to track both the loss of nodes and the addition of unverified nodes to the network.

Although this system increases the amount of time needed for the control node to recognize the disappearance of a node from regular network traffic, it also allows some leeway for network interference. If a node misses one or two cycles due to transient noise or ambient interference, the control node accounts for that slight break in transmissions, and the node is able to remain within the network as an authorized entity.

D. Node Authentication

To protect the network against infiltration by outside entities, we have designed a Node Authentication scheme that works in conjunction with the Network Topology solution.

The solution used in this work is a ‘Challenge-and-Response’ scheme which is triggered whenever a new node joins the network. State diagrams for both for the control node and for a sensor node requesting authentication are shown in Figure 8. The challenge and response scheme causes a slight decrease in network throughput since it requires a pause in normal network operation to perform each check.

The Challenge-and-Response sequence is triggered when a new node joins the network. Thus, the Node Authentication and Network Topology schemes are closely tied in both functionality and implementation. If the Network Topology scheme detects the presence of a new node in the network, it sets an internal flag which initializes the Node Authentication scheme.

The control node pauses network operation before the beginning of the next cycle and sends a command to the node in question indicating the beginning of a Challenge-and-Response routine. If the control node does not receive an acknowledgment (ACK) from that node, then the control node times out and determines the node in question to be untrusted. Should the control node receive an ACK from the sensor node within the set time frame, both nodes then switch to a private encryption key in order to ensure secure communication. This procedure also serves to leverage the symmetric key encryption scheme as an additional identity check.

Once both nodes have switched to the private key value, the control node will use a nonce to verify the sensor node’s authenticity. A nonce is simply a randomly generated sequence of bytes which the sensor node in question must correctly receive from the control node’s encrypted transmission and return. The control node then sends an ACK to the sensor node indicating successful receipt of its message and both nodes then return to the main network KY setting. Finally, based on the results of the Challenge-and-Response check, the control node will broadcast a message to the network indicating that the oncoming node has been authenticated and can be trusted. The control node and all authenticated sensor nodes then resume regular network activity.

Figure 8. State Machine showing logic for Node Authentication in Control and Sensor Nodes.
V. IMPLEMENTATION RESULTS

In this section, we discuss the methodology and results of two field tests conducted to verify implementation of both the functionality of the RTI wireless sensor network’s vehicular detection capabilities and the associated security scheme described in Section IV.

A. RTI Functionality Test

To collect information on the baseline functionality of the RTI WSN, the project team conducted an 18 node field test of the network in the parking lot of the Navy-Marine Corps Memorial Stadium. The purpose of the field test was to observe the RTI network operation and verify that it was capable of distinguishing between dissimilar vehicle profiles.

Nodes were set up in two parallel rows with a distance of 10 meters between rows. There was a separation of 1.0 m between each node in a row. A control node and listening node were stationed at either end of the network. The two vehicles used for the test, a large utility van and a small electric car, are both shown in profile at the top of Figure 9.

The test itself consisted of taking RSS readings of a vehicle at three positions within the network. Additionally, readings were taken of the test vehicle moving through the network at a slow speed. These tests were repeated for both the utility van and electric car. Data was later processed in MATLAB via an algorithm described in the work of Martin et al [11].

Shown in Figure 9 is a side by side comparison of the radio tomography profile created by the utility van and electric car, respectively, at different points within the network. The data provides clear differentiation between the two test vehicles and validates the sensor network’s primary objective.

B. Security Functionality Test

A second test was organized to verify the implementation of the network security system. Sample testing was performed on the Jamming Mitigation, Network Topology, and Node Authentication schemes.

Testing took place in a lab setting using a smaller 6 node WSN in order to simplify network functionality for testing. The smaller network size was satisfactory, since vehicular identification capabilities were not considered in the testing and the higher resolution of a larger network was not needed. Separate tests were conducted for each security scheme using nodes programmed with code specifically for that respective scheme.

Testing on the Network Topology implementation consisted of deactivating and reactivating sensor nodes while the network was running to simulate nodes dropping off of and entering the network. These checks were performed in groups of one, two, and three nodes at a time. The data output of the network was recorded through a listening node. This data was used to verify that the control node was able to accurately identify both a sensor node drop and the entrance of a sensor node to the network. Out of 150 trials, the control node succeeded in correctly detecting 88.7% of both node deactivations and activations. Figure 10 shows a summary of the test results. The results presented here indicate a robust ability to identify sensor node departures from and entrances to the network. It should be noted that following these tests it was discovered that one of the XBee modules was set in an unexpected condition which, after powering down and reactivating the node, caused the node not to experience an expected delay in data transmission. Thus, the sensor node was never noticed by the control node as having been dropped. In the absence of this issue, our results would have yielded even higher success percentages.

Testing of the Node Authentication scheme was conducted using a similar methodology. In this battery of tests, the sensor nodes were configured to implement the Node Authentication code including predetermined public and private keys. A portion of the sensor nodes were pre-assigned valid keys, while the remaining nodes were pre-assigned invalid keys. The recorded network traffic data was used to verify that the control node’s ability to correctly distinguish between authorized and

![Figure 9. Resulting Radio Tomography profile for utility van (left) and electric car (right) within the network.](image)

![Figure 10. Performance of Network Topology scheme implementation. Shows the number of nodes entering and exiting the network detected by the control node, compared to the number of node detections expected.](image)
unauthorized nodes. Out of over three hundred trials, 99.0% of
the authorized nodes entering the network were correctly
identified, and 100% of the unauthorized nodes were correctly
identified. The test results are summarized in Figure 11. Our
results indicate that the implemented Challenge-and-Response
based Node Authentication scheme is capable of protecting
network integrity against unauthorized nodes, even when
multiple nodes are entering and exiting the network simultaneously.

The Jamming Mitigation security scheme was tested by
recording network traffic for a predetermined length of time
while we simulated broadband jamming across a number of
channels. The jamming signal was created using an Agilent
ESG-D signal generator transmitting an FM modulated signal
at 19 dBm (the XBee RF modules are capable of transmitting at
up to 18 dBm). The network was configured to frequency hop
across three of the available preset channels and network traffic
was recorded while jamming was present across zero, one, and
two channels respectively. Listening nodes were configured to
monitor all 3 active channels simultaneously.

Implementation efficiency was evaluated based on resulting
network throughput, as measured by the ratio of the number of
active links and packets received versus the expected number
of active links and received packets. A link was considered
inactive if it was reported by a node as being dropped (i.e. the
node was not able to determine an RSS value for that link
during the previous scan) or if the data packet in which the link
would have been reported was dropped. As anticipated, the
resulting throughput of this test decreased in direct correlation
to the number of channels jammed, as shown in Figure 12. The
total number of packets dropped as a function of time was also
recorded through the jamming mitigation tests. Figure 13
shows these recorded values under each of the tested jamming
conditions. Using these figures, we observed that there was a
linear correlation, which remained constant across time,
between network throughput and the intensity of jamming
present (i.e. the number of channels experiencing jamming).
The number of dropped packets in each test can be referenced
against the ~3800 total data packets expected to be received
across the course of each test.

In low noise environments, the frequency hopping scheme
operates effectively without dropping an excess number of
packets. Although only three channels were used in our sample
tests, our results indicate that limited signal interference could
be effectively overcome by utilizing a larger number of active
channels.

In this paper, we have proposed and fielded a secure
ZigBee-based wireless sensor network capable of vehicular
detection and identification using radio tomographic imaging.
The RTI WSN is comprised of readily available components
and is easily configured. The network is capable of
distinguishing between distinct vehicle profiles and can be used
in a number of public safety, military, or commercial
applications.

Field results indicate that our design is capable of
maintaining network functionality despite moderate noise
interference and is resistant to a number of common network
infiltration attacks. This design is applicable to any similar
ZigBee-based WSN utilizing a central controller. Furthermore,
the principles of our implementation could reasonably be used
to increase the network security resilience of any WSN
configured in a mesh network topology with a central
controller.

VI. CONCLUSIONS

Figure 11. Number of sensor nodes properly authenticated upon activation
using implemented Node Authentication scheme. Divided into categories of
authorized and unauthorized sensor nodes.

Figure 12. Throughput measured by received data packets and number of
active links using implemented Jamming Mitigation scheme under varying
levels of interference.

Figure 13. Comparison of total number of data packets dropped across time
under different levels of jamming interference.
REFERENCES


