The University of Kansas

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

Technical Report

TRANSPORTATION SECURITY SENSOR NETWORK: SENSOR SELECTION AND SIGNAL STRENGTH ANALYSIS

Angela Oguna

ITTC-FY2010-TR-41420-17

December 2009

Project Sponsor:
Oak Ridge National Laboratory

Abstract

Cargo theft is a major problem in the US; the FBI estimated losses of $15-30 billion in 2006. The Transportation Security Sensor Network (TSSN) aims to mitigate these risks by utilizing sensors that will track and monitor train-borne shipping containers. Prior to deployment, we need to know the read ranges of proposed sensors and their practicability in a rail scenario. I describe the experiments that were performed to test the sensors; results indicate that the wire sensor is the most suitable. Ultimately, I expect that the improved cargo security resulting from TSSN implementation will lead to fewer incidences of theft, thereby lowering prices for the final consumer.

CONTENTS

I Introduction 1

II System Architecture 1

II-A Mobile Rail Network 1

II-B Virtual Network Operations Center 3

II-C Trade Data Exchange 3

III Tests 3

III-A Read Range Tests 3

III-A1 Free Space Tests 3

III-A2 Tests in the presence of a Ground Plane 4

III-A3 Test with Cars 4

III-A4 Test on a Trailer 4

III-B Short-haul Rail Trial 4

IV Results 4

IV-A Read Range Tests 5

IV-A1 Free Space Tests 5

IV-A2 Tests in the presence of a Ground Plane 5

IV-A3 Test with Cars 5

IV-A4 Test on a Trailer 6

IV-B Short Haul Train Test 6

IV-B1 TSSN Component Interaction 6

IV-C HSDPA Signal Strength 6

V Conclusion 7

Acknowledgments 7

References 8

LIST OF FIGURES

1 Transportation Security Sensor Network (TSSN) Architecture 2

2 Mobile Rail Network Hardware 2

3 Wireless Sensors 3

4 Read Range Success versus Seal-Reader separation in free space 5

5 Read Range Success vs. Seal-Reader Separation 5

6 Read Range Success versus Seal-Reader Separation in Presence of Cars 6

7 HSDPA Signal Strength vs. Time 7

LIST OF TABLES

I Number of Messages Generated by TSSN Components 7

I. INTRODUCTION

CARGO shipments are subject to theft, hijacking, and tampering. In 2006 the FBI estimated that cargo theft cost the US economy between $ 15–30 billion in annual losses [1]. However, law enforcement acknowledges that these values are only about 40% of the losses that occur; due to the reluctance of businesses to report theft. Cargo is also used as a guise to transport illegal drugs, arms, and aliens; giving rise to other forms of crime that law enforcement officers tackle daily. Indirect costs stemming from cargo crimes, such as delayed deliveries, insurance claims and processing, and in the worst case scenarios injuries or loss of life, result in total losses that are 4-5 times greater than the direct losses [2]; a cost that the consumer eventually carries.

Cargo transportation requires a complex interaction between the originator, the shipper and the receiver. This paper describes two components of a system designed to minimize the effects of cargo crime. The transmission ranges of the sensors used will be measured to design and deploy the system. The Global System for Mobile (GSM) communications signal strength along a train route will be collected to guide the future design of algorithms that switch between communication routes.

A hardware and software system referred to as the Mobile Rail Network (MRN) monitors the cargo in transit. The Mobile Rail Network sends alerts to the Virtual Network Operations Center (VNOC), which processes the messages to determine if the shipper and/or recipient should be notified. The VNOC communicates with the Trade Data Exchange (TDE) to get information on the cargo shipment, and determine the personnel to be informed of the security alert. Therefore, the Mobile Rail Network, Virtual Network Operations Center, and the Trade Data Exchange link the originator, the shipper and the receiver; ensuring that informed decisions can be made in a timely manner in case of a security breach.

This paper describes the component interaction within the TSSN and experimental data documenting suitable hardware for a rail environment. The results show that the TSSN can effectively monitor cargo, and notify decision makers of security breaches. The rest of the paper is laid out as follows: Section II , describes the TSSN architecture and its components. Section III discusses two experiments to determine suitable hardware for a rail environment, and also assesses the effectiveness of the TSSN system in cargo monitoring. Section IV describes the results of our tests and finally Section V describes the conclusion.

II. SYSTEM ARCHITECTURE

A Transportation Security Sensor Network (TSSN) was set up to achieve the objectives stated above. The TSSN utilizes a Service Oriented Architecture (SOA) to provide a reusable framework that can be implemented across the transportation industry [3]. It uses open web standard interfaces, such as Apache Axis 2, to process and share information across different applications. The main components of the TSSN are the Mobile Rail Network (MRN), Virtual Network Operations Center (VNOC), and the Trade Data Exchange (TDE), which allow interaction between the originator, shipper, and receiver as illustrated in Fig. 1.

A. Mobile Rail Network

The Mobile Rail Network (MRN) includes the software and hardware that monitor freight on the train and report any suspicious activity to a Virtual Network Operations Center (VNOC). The hardware component of the MRN consists of a set of wireless shipping container security sensors positioned on individual containers, an electronics suite located in the locomotive, and a set of antennas that is magnetically mounted on the locomotive roof to maximize reception. The electronics suite contains a computing platform, a power inverter, a three-axis accelerometer, a security seal interrogation transceiver and wireless data modems as illustrated in Fig. 2

The MRN software consists of the MRN SensorNode, the MRN AlarmProcessor and a communications service. If the seals are tampered with, they send an alert burst message to the MRN SensorNode. The MRN SensorNode service determines the seal events that are unsafe and it sends an alert message to the MRN AlarmProcessor service for each suspicious event. The MRN AlarmProcessor performs further

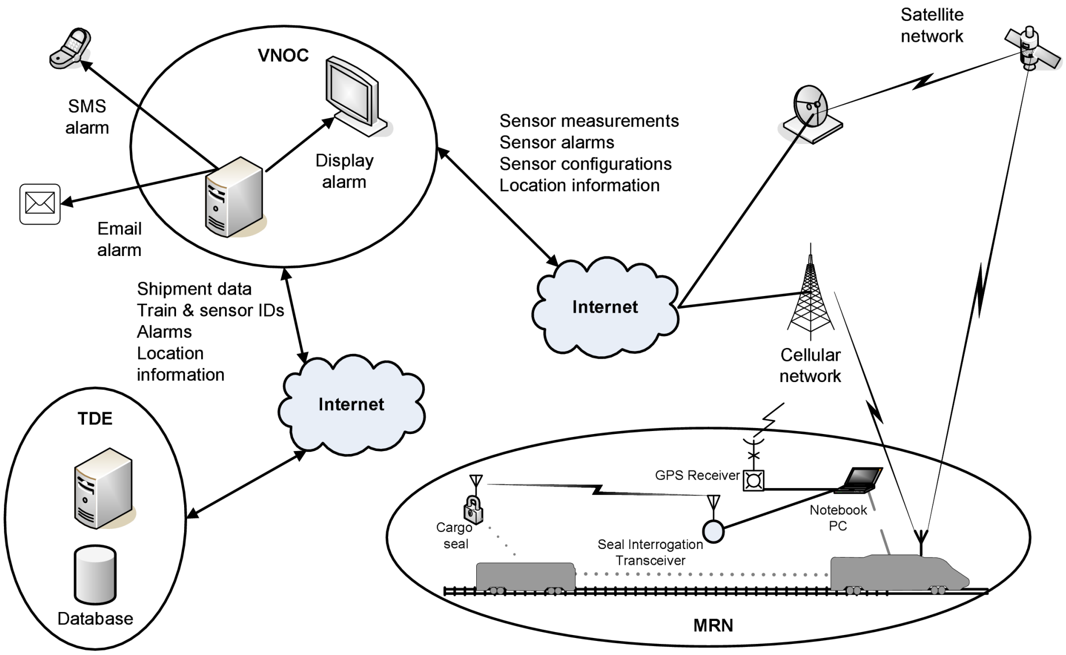


Fig. 1. Transportation Security Sensor Network (TSSN) Architecture

processing on the alert and sends an MRN alarm message to the VNOC AlarmProcessor if the event is indeed unsafe. The communications service logs the High Speed Downlink Packet Access (HSDPA) signal strength-information that will determine when the communications system should switch between the Iridium satellite and Global System for Mobile (GSM) communication connection.

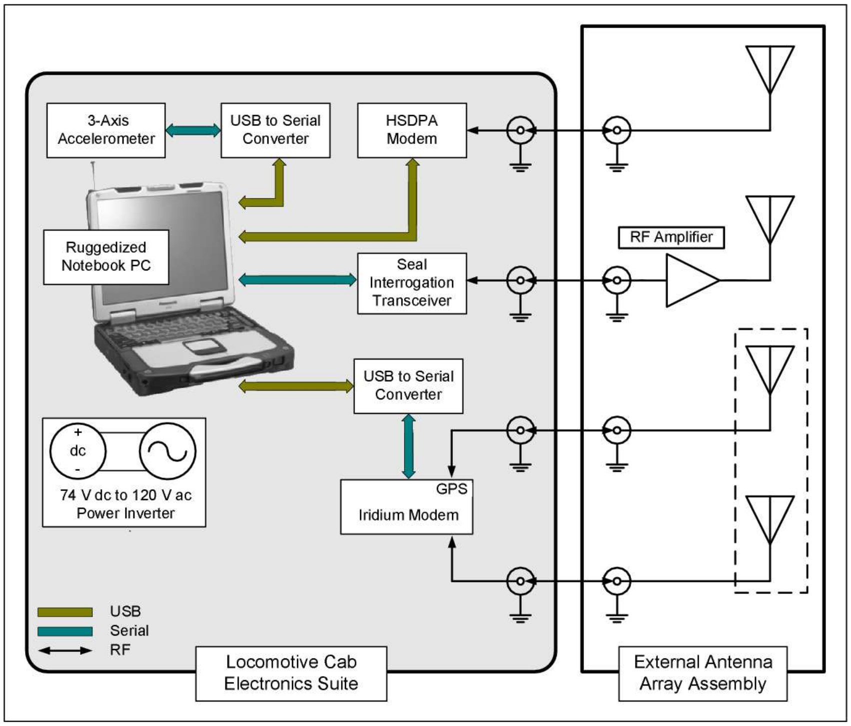


Fig. 2. Mobile Rail Network Hardware

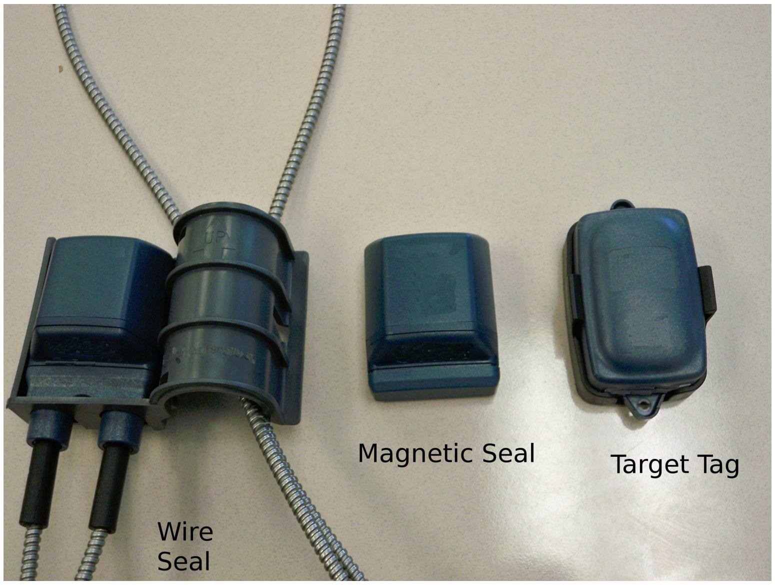


Fig. 3. Wireless Sensors

B. Virtual Network Operations Center

The Virtual Network Operations Center (VNOC) contains a VNOC AlarmProcessor and a VNOC AlarmReporting Service which run on a remote server at the monitoring location. The VNOC AlarmProcessor receives alarms from the MRN AlarmReporting Service. It queries the Trade Data Exchange for cargo information and uses the response to determine if a VNOC alarm should be forwarded to personnel. The MRN alarm and shipment data are combined into a message that is sent to the user by the VNOC AlarmReporting Service via email and/or SMS. The VNOC also transmits startMonitoring, stopMonitoring, and getLocation commands from the TDE to the MRN.

C. Trade Data Exchange

The Trade Data Exchange (TDE) contains the cargo information, which it relays when queried by the VNOC about specific shipments. It also stores alarm messages sent to the user by the VNOC in addition to sending startMonitoring, stopMonitoring, and getLocation commands to the MRN via the VNOC.

III. Tests

Two sets of experiments were conducted to test the TSSN hardware. The first set of experiments analyzes the performance of the sensors in a static environment, while the second set of tests records the High-Speed Downlink Packet Access (HSDPA) signal strength and evaluates the overall TSSN performance.

A. Read Range Tests

The primary objective of this test was to determine which wireless seal provided the best read ranges, and would best withstand a rail environment. The magnetic seal, target tag and the wire seal, illustrated in Fig. 3, were tested in free space, in the presence of metal ground plane, near cars and next to a trailer.

1) Free Space Tests: The seal interrogator transceiver (SIT) and the magnetic seal were placed on plastic carts to elevate them and minimize grounding effects. The SIT antenna was placed at a fixed position, while the seal was moved away from the SIT antenna in 10 m increments. The seal was interrogated ten times at each new seal position, and then the seal-SIT antenna separation was incremented by a distance of 10 m. Responses received within two minutes were recorded as successes; otherwise they were counted as failures. The procedure was repeated until the maximum read distances for each seal was reached or exceeded.

A line of sight path existed between the SIT antenna and the seal during the test. Both the SIT reader and the laptop remained powered for all the tests, except for the test performed on the trailer because their battery power could only last 1.5 hours before shutting off.

2) Tests in the presence of a Ground Plane: The objective of this test was to determine the effect of a metal ground plane on the read range. The same procedure outlined in free range test was followed, but the seal interrogator transceiver was placed on 1.5 m × 0.9 m metal sheet. Ten readings were taken as before and the tests were repeated until the maximum read range was obtained, or the number of successful readings fell below two. The tests were repeated with the SIT antenna placed on the metal sheet, and the seal positioned on a Styrofoam block covered with aluminum foil to determine the effects of placing both the seal interrogator transceiver and the seal on metal ground planes.

3) Test with Cars: The objective of this test was to test the effect of large interfering metal objects on the read ranges. The seal interrogator transceiver was positioned on a cars trunk lid. The seal was placed on a 0.9 m high wooden block one car width away from the reader. Unlike previous tests, there was no direct line of sight path between the seal interrogator and the seal. Ten readings were taken as before at each position, and the seal was then moved one parking spot (2.5 m) farther away. The tests were repeated until the number of successful readings dropped to two.

4) Test on a Trailer: The final test was performed on a 16 m trailer to simulate a rail environment. A car was parked in front of the trailer and the SIT antenna was placed on the cars roof while the seal was placed at the back of the trailer. Ten queries were sent out by the seal interrogator as in the previous tests and if no response was received within two minutes, the interrogation was counted as a failure. There was no line of sight path between the seal and the seal interrogator, and both the seal interrogator and laptop were running on battery power.

B. Short-haul Rail Trial

This test was carried out on a train traveling on a 35 km route from an intermodal shipping facility to a rail yard. The main objectives were to analyze message transmission between the TSSN components for correctness and monitor the HSDPA signal strength to determine the feasibility of switching between an Iridium satellite and HSDPA link to relay messages between the MRN and the VNOC. During the test, the VNOC was located at the university (approximately 60 km away), the TDE was at a remote location approximately 48 km away, and the MRN was located in the locomotive cab. Several seals were hung on intermodal containers, and one seal was kept in the locomotive cab with the MRN electronics suite. The latter seal was opened and closed to simulate seal open and close events. The VNOC AlarmProcessor received alerts from the MRN which contained the event time, seal position, message type, unique sensor ID and the event type. The VNOC AlarmProcessor queried the TDE to obtain the shipment information and decided (based on a set of rules) if personnel should be notified. If the alarm met the set criteria, the MRN alert and the shipment data were combined into an email or SMS message that was sent to the user by the VNOC AlarmReporting service. The GSM signal strength between the MRN and the VNOC was monitored and recorded in log files by the communications service. The experiment was considered a success as all the events detected by the seals were processed and reported to the personnel using email and SMS.

IV. Results

This section discusses the results of the TSSN hardware evaluation and the HSDPA signal strength experiment, in addition to presenting brief results on overall TSSN performance.

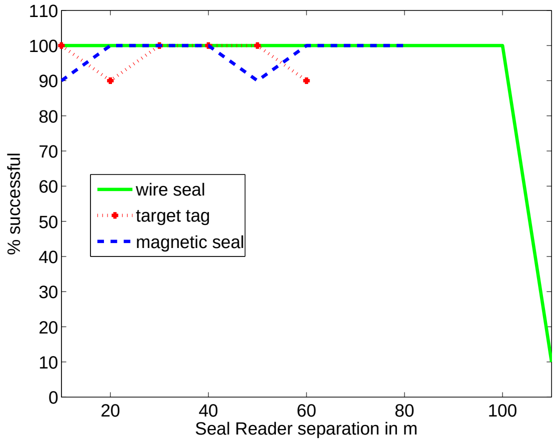
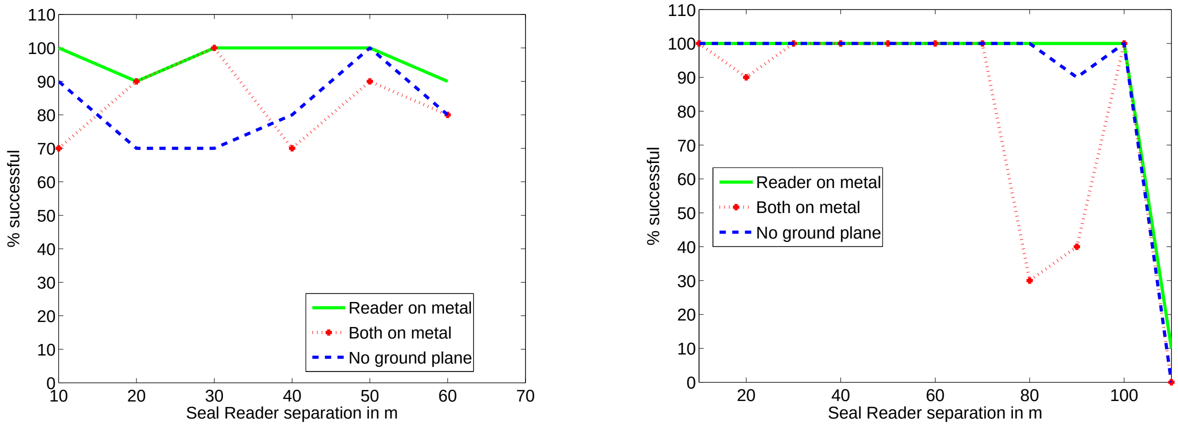


Fig. 4. Read Range Success versus Seal-Reader separation in free space



(a) Target Tag

(b) Wire Seal

Fig. 5. Read Range Success vs. Seal-Reader Separation

A. *Read Range Tests*

1) Free Space Tests: The highest percentage of successful readings was obtained in the free space tests which were characterized by a direct line of sight in the duration of testing. The wire seal had the longest read range (100 m) followed by the magnetic seal which could be read up to 90 m, contrary to manufacturers specified range of 50 m. The target tag achieved its stated read range of 50 m. The results illustrated in Fig. 4 show the superior performance of the wire seal, as it recorded 100% success rate throughout the test.

2) Tests in the presence of a Ground Plane: The performance of both the magnetic seal and the target tag seals deteriorated when a ground plane was introduced in the testing environment. Their performance further declined when both the SIT antenna and the seals were placed on ground planes in comparison to the scenario where only the SIT was positioned on a ground plane. Fig. 5a illustrates the performance of the target seal when tested with and without a ground plane.

The wire seal performance was not affected greatly by the ground plane especially at shorter distances as shown in Fig. 5b. Although a lower performance is noted as the seal approaches its maximum read range, it clearly displays a superior performance when compared to the target tag and magnetic seal.

3) Test with Cars: The wire seal and target tag performed well at short distances when tested with cars. However, their performance declined as the separation distance was increased. A lower success rate had been expected for the target tag and magnetic seal due to the ground planes introduced by the car bodies. The poor performance for the wire seal could be attributed to the lack of a line of sight path in

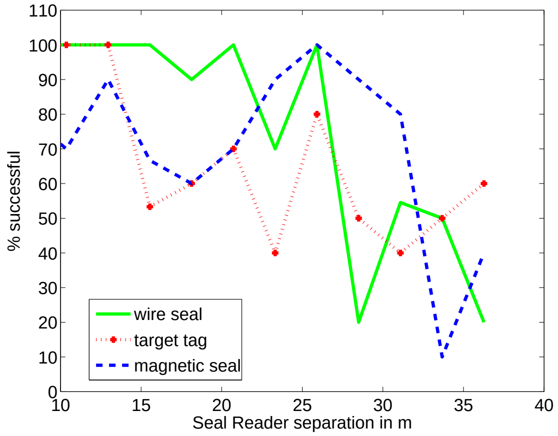


Fig. 6. Read Range Success versus Seal-Reader Separation in Presence of Cars

this experiment. Furthermore, the tests were carried out in an open parking lot, while the previous tests had been performed next to several large buildings. This indicates that the seal performances in the initial tests may have been improved by signal reflection from the surrounding buildings. Fig. 6 displays the performance of the seals in the presence of cars.

4) Test on a Trailer: The final test involved testing the seals when attached to the end of a 16 m (53') trailer. This time there was no line of sight path between the seal and the seal interrogator, and the open location minimized reflection from surrounding buildings. The percentage of successful readings recorded with the target tag, wire seal and magnetic seal were 0%, 20%, and 10% respectively. The decreased performance was partly attributed to the absence of a line of sight path between the SIT reader and the seal, as well as a lower transmit power since the seal interrogator transceiver was running on battery power. However, more tests are needed to confirm our assertions. The wire seal displayed a better performance than the magnetic seal and the target tag; making it most suitable for the rail environment.

B. Short Haul Train Test

1) TSSN Component Interaction: Table I shows the messages that were transmitted between several TSSN components. All VNOC queries were responded to by the TDE, i.e., 63 shipmentQueries and 63 shipmentQueryResponses, and the MRN responded to all commands from the TDE which were sent via the VNOC. This illustrates that all three TSSN components could communicate successfully without messages being dropped. Table I also illustrates that some messages are filtered by the system. The MRN SensorNode reported 546 alerts to the MRN AlarmProcessor. Only 131 alerts met the criteria set by the rules in the MRN AlarmProcessor and were sent out as MRN alarms to the VNOC AlarmProcessor. All the MRN alarms were sent out as VNOC alarms; indicating that they met the set criteria, and were therefore, sent out as SMS or email messages to decision makers [4]. Our results confirmed that the TSSN could not only detect unsafe events, but it could process the messages and relay the information to decision makers.

C. HSDPA Signal Strength

In the current TSSN implementation the MRN is instructed, at startup, to either use an Iridium satellite or HSDPA link to transmit messages between the VNOC and the MRN. Future TSSN implementations will have an algorithm that can switch dynamically between HSDPA and satellite link transmissions.

The MRN communications service monitored HSDPA signal strength during the short-haul trial. Fig. 7 provides a trace of the change of signal strength with time. The signal strength is constant at the beginning of the trip. This corresponds to the time when the MRN was on, but the train was stationary. There are

TABLE I
NUMBER OF MESSAGES GENERATED BY TSSN COMPONENTS

Message Type	From	To	No. of Messages
Alerts	MRN SensorNode	MRN AlarmProcessor	546
MRN Alarm	MRN AlarmProcessor	VNOC AlarmProcessor	131
VNOC Alarm	VNOC AlarmProcessor	VNOC AlarmReporting	131
getLocation	TDE	MRN SensorNode	30
Location	MRN SensorNode	TDE	30
shipmentQuery	VNOC AlarmProcessor	TDE	63
shipmentQueryResponse	TDE	VNOC AlarmProcessor	63

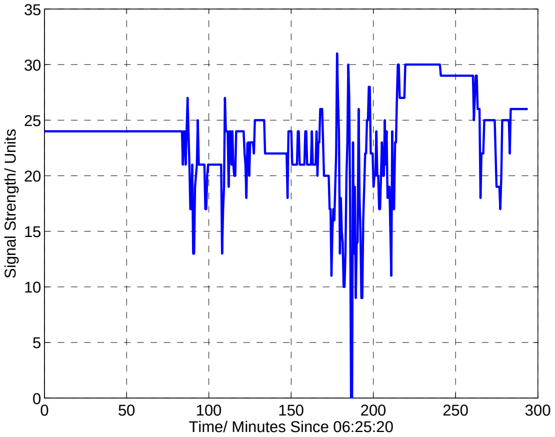


Fig. 7. HSDPA Signal Strength vs. Time

two other constant portions at about 220 and 240 minutes when the train stopped at a train crossing. Once the train journey begins, the signal strength varies between 18 and 24 units. For the greater part of the journey, the signal strength is reliable except at the 180th minute when the signal strengths drops to 0. This illustrates the viability of a dual communication system that switches between the HSDPA and Iridium link in areas with a strong HSDPA signal strength. The more expensive iridium satellite could be turned on in areas with low HSDPA signal.

V. CONCLUSION

This paper presents results from hardware testing and a short haul trial of the Transportation Security Sensor Network (TSSN). The wire seal was the most practical sensor for a rail environment since it had a long read range, and was not affected greatly by metal surfaces. A strong HSDPA signal was detected along the train route, although this result does not generalize to other train routes, it was useful information for interpreting other results of this experiment. In addition, the collected HSDPA signal strength data will be used in the future design of an algorithm that can dynamically switch between modes of communication. Although the TSSN system can effectively monitor cargo, and transmit messages to decision makers; a lot of messages were dropped at the MRN AlarmProcessor. Given the large number of filtered messages, it is important to perform further analysis to see if the rules that determine unsafe events are incorrectly dropping important messages. This early test of the TSSN provides evidence that this design can be efficient in streamlining the communication between the originator, shipper, and the recipient to ensure safer cargo transportation. By reducing the risks of cargo theft, we hope that this will result in monetary savings for manufacturers that will eventually trickle down to the final consumer through lower prices.

ACKNOWLEDGMENTS

This work was supported in part by Oak Ridge National Laboratory (ORNL)—Award Number 4000043403.

References

[1] Federal Bureau of Investigation. (2006, July 21) Cargo Theft's High Cost. Headline. Federal Bureau of Investigation. [Online]. Available: http://www.fbi.gov/page2/july06/cargo_theft072106.htm

[2] R. J. Fischer and G. Green, *Introduction to Security*, 7th ed. Boston, MA: Butterworth-Heinemann, 2004.

[3] K. Martin, "Service Oriented Architecture for Monitoring Cargo in Motion along Trusted Corridors," University of Kansas, Lawrence, KS, ITTC Tech. Rep. ITTC-FY2010-TR-41420-13, July 2009.

[4] D. T. Fokum *et al.*, "Experiences from a Transportation Security Sensor Network Field Trial," University of Kansas, Lawrence, KS, ITTC Tech. Rep. ITTC-FY2009-TR-41420-11, June 2009.