Service Oriented Architecture for Monitoring Cargo in Motion Along Trusted Corridors

V. S. Frost, D. T. Fokum, M. Kuehnhausen, M. Zeets, L. S. Searl, E. Komp, D. DePardo, A. N. Oguna, G. J. Minden, J. B. Evans, B. Quanz, H. Fei
(fokumdt@ittc.ku.edu)

Introduction

- Emerging need to monitor cargo along corridors from port to inland intermodal facility.
- Disparate complex systems are used today in the container transport chain leading to a lack of visibility, accountability, efficiency, and security.
  - Deficiencies in these areas expose the system to attacks such as:
    - The Trojan horse (the commandeering of a legitimate trading identity to ship an illegitimate or dangerous consignment);
    - Hijack or theft of goods;
    - Transport of dangerous goods
  - Insufficiencies in these areas must be overcome by creating secure trade lanes (or trusted corridors) especially at intermodal points, e.g., at rail/truck transitions
  - Research and development is underway to realize the vision of trusted corridors.
- The proposed research focuses the general themes: advanced communications, networking and information technology applied to creating trusted corridors.
- Objective of the research is to provide the basis needed to improve efficiency and security of trade lanes by combining real-time tracking and associated sensor information with trade data exchange information.
- Several crucial research questions that must be answered in order to attain this objective, e.g., how to create technologies that will allow continuous monitoring of containers leveraging communications networks as well as trade and logistics data within an environment composed of multiple enterprises, owners, and operators of the infrastructure.
  - Research is needed to address these questions
  - Present initial results of experiments with a Transportation Security Sensor Network (TSSN) that can be used to provide visibility into cargo shipments.

System Architecture

- TSSN system is composed of three major geographically distributed components.
  - Mobile Rail Network (MRN) consists of:
    - container seals that communicate with a reader over a wireless network when an event occurs.
      - Events include seal opens, missing seals, or low battery warnings.
    - Sensornet collector node that interfaces with the reader, processes events, determines which events need to be communicated, and chooses the mode of communication (e.g., GSM or satellite) to a virtual network operations center (VNOC).
  - Virtual Network Operations Center (VNOC) runs on a server. It:
    - accepts messages from the MRN
    - obtains associated cargo information from a remote trade data exchange (TDE)
    - combines cargo information with MRN event report to form an alarm message that is sent (by e-mail or SMS) to appropriate decision makers.
  - Trade Data Exchange (TDE) is hosted on a remote server. It:
    - Contains shipment information
    - Responds to shipment queries from the VNOC
- Architecture is based on already existing components as well as those developed especially for this effort
  - Infrastructure is based on W3C and OASIS web services specifications
  - Services are described using Web Service Description Language (WSDL)
  - Client/Server communication is based on Simple Object Access Protocol (SOAP)
  - Figures 5 and 6 show the architecture diagrams for the MRN and VNOC respectively.

Experiments

- Experiment 1 (Using pick-up trucks)
  - MRN sensor node and reader were located in one truck. Seals were placed in a second truck driven behind the first.
  - VNOC was located in Lawrence, KS and TDE in Overland Park, KS
  - When the VNOC received alarms from the MRN, cargo information was retrieved from TDE
    - VNOC combined information that was communicated to interested parties
    - VNOC also performed complex alarm processing to filter alarms based on geo-location and time
  - Experiment Results:
    - All open and close events were reported as expected; however, reporting times varied from what was expected due to clock skew between MRN and VNOC.
    - Network, sensors and readers performed reliably, and reader only failed to read sensors when trucks were about 400 m apart.
    - Figure 1 shows a trace of experiment route with events overlaid on Google Maps.
    - Pink tear drops indicate an open event, green tear drops a close event, pink tacks indicate a lost GPS signal, green tacks a lock on a GPS signal, a red exclamation point indicates where GSM connectivity was lost and a green arrow indicates where GSM connectivity was regained.

Fig. 1 Route and event locations from first field experiment

- Experiment 2 (Short-haul Rail Trial)
  - Experiment objective was to determine the suitability of the TSSN software for detecting tamper events on intermodal containers. We were also to investigate if decision makers could be informed of events using SMS messages and emails.
    - VNOC and TDE remain in locations as described above.
    - MRN sensor node and reader were placed in one locomotive and used to monitor five seals placed on containers and in the locomotive
    - Train proceeded along a 22 mile route from intermodal facility to a rail yard.
    - Experiment was a success, as events were detected on seals and reported to decision makers.
    - Detailed log files were collected from experiment and are being post-processed
    - Figure 2 shows the configuration used in the short-haul rail trial.

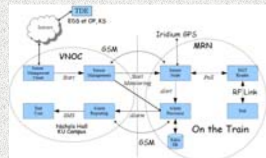

Figure 2 Short-haul rail trial configuration

- Sample alarm email:


NOC AlarmReportingService
Date-Time: 2009 01 07 07 12 17 CST / 2009 01 07 13 12 17 UTC
Lat/Lon: 38.83858 -94.56186, Quality: Good

TrainId=ShrtHaul1
Severity: Security
Type: SensorLimitReached
Message: SensorType=Seal SensorID=IAHA01054190 Event=Open Msg=
NOC Host: laredo.ittc.ku.edu

Shipment Data:
Car Pos: 3
Equipment Id: EDS 10970
BIC Code: ITTC054190
STCC: 2643137

Initial Results from Post-processing of log files

- Post-processing done using a Java library (LogParser) developed in-house.
  - LogParser library allows parsing of the log files generated by the LogModule.
    - Library reads in all available information (time, message size, from and to address) including:
      - original SOAP message.
      - Message couples (SOAP request and responses)
      - Transmit/receive message pairs
    - All information contained in the SOAP message itself can be evaluated using XPath expressions.
  - Library uses couples and transmit/receive message pairs to relate messages for post-processing.
- Fig. 3 shows a trace of GSM signal strength versus time in seconds from the start of the rail trial, while Figure 4 shows request/response times for messages originating at the VNOC for the MRN

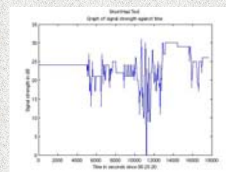

Fig. 3 GSM Signal Strength versus time

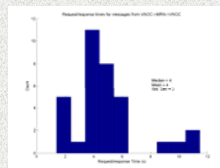

Fig. 4 Request/response times in seconds for messages from VNOC to MRN

Conclusion

- Work is ongoing to post-process the log files from the rail trials.
- More work is needed to improve the time synchronization on the MRN sensor node.
- TSSN is viable for monitoring cargo on trains.
  - Further research is needed to address issues including:
    - Operating radios and wireless networks in harsh environments
    - Achieving adequate quality of service from end-to-end networks
    - Optimum placement of sensors and communications devices on trains
    - Security and management mechanisms for the constituent components of the TSSN
- Desired result of research is a standards-based open environment for cargo monitoring with low entry barriers to enable broader access by stakeholders while showing a path to commercialization.

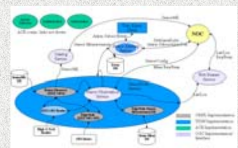

Fig. 5 Mobile Rail Network Architecture

Fig. 6 Virtual Network Operations Center Architecture