The University of Kansas

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

Technical Report

# Phase One Report: A Unified Architecture for SensorNet with Multiple Owners

Gary Minden, Victor Frost, David Petr,
Douglas Niehaus, Ed Komp, Daniel Fokum,
Pradeepkumar Mani, Andrew Boie,
Satyasree Muralidharan, and James Stevens

ITTC-FY2008-TR-41420-06

December 2007

Project Sponsor:
Oak Ridge National Laboratory (ORNL)
Award Number 4000043403

# Abstract

Many groups have identified sensor networks as a technology that can contribute to the national need to monitor and detect threats. Most of the work on sensor networks focuses on a wireless network to interconnect sensors and convey telemetry data to a collection point. While the underlying radio and communications technology are prerequisites and still pose problems, a holistic view is needed to ensure that the right information gets to the right people at the right time; this requires an integrated and interoperable architecture. The system considered here is consistent with the ORNL's SensorNet Information Architecture and goes beyond basic telemetry collection to incorporate assured and controlled access to sensor network assets; implying a focus on security and management mechanisms.  An important aspect of the system developed here is that it does not assume a single entity owns and operates the complete network. Many of the component technologies for a comprehensive sensor network exist. However, robust techniques for integrating the component technologies into a comprehensive sensor network system present significant challenges. This effort addressed the issues of interfaces between sensor network components and domains, authorization/authentication as well as addressing distributed command and control loops composed of data collection, data analysis, and actuator elements. A prototype was developed, implemented, and evaluated. The lessons learned from the implementation of a prototype contribute to the continued development of sensor networks.  Issues related to secure routing, multi-hop wireless networks, and hardware platforms for sensor networks were also addressed. The next step is to identify a suitable environment in which to test and evaluate the technology. Specifically, the applicability of the technology to rail system monitoring was pursued to expand the developed technologies to a testbed targeted to improve and monitor railroad transportation of hazardous cargo focusing on transporter identification, real-time monitoring and tracking, safety and compliance.

# Table of Contents

# List of Tables

# 1 Overview

Sensor networks have been identified as being key technology in monitoring and detecting threats. These systems face critical technical challenges in providing a security and management architecture in scenarios representative of a large class of applications. The design and architecture of sensor networks [1], [2] and [3] have been studied and many networks have already been deployed [4]. Past efforts addressed the design issues of various component technologies of sensor networks. PicoRadio [5] and SmartDust [6] focused on system level issues in designing sensor hardware. LEACH [7] focused on network layer design issues for these networks. Other works like SensoNet [8] and WINS [9] recommend an entire protocol stack for sensor systems. Relatively few systems include a model for sophisticated information dissemination systems that could be based upon the underlying sensor network technologies, for example [8]. As sensor networks progress toward widespread deployment, the security issues involved assume increasing importance. Many early protocols like SNEP, µTesla [11] and Tesla [12] were proposed as building blocks to provide standard security functions for these networks. While some efforts (e.g., [13]) focused on security solutions used for mobile user devices in the context of sensor networks, efforts like [14] considered a variety of approaches for key distribution in sensor networks where the overhead of these protocols on a variety of hardware platforms was analyzed. Various research efforts were directed toward providing low-end devices by integrating cryptographic primitives with low cost microcontrollers. For example: AVR controllers [15] and the Dallas iButton [16] support primitives for public key encryption, together with a possibility for modular implementation. The above studies focused mainly upon the security functions that can be built inside a sensor node. They do not consider a broader security infrastructure for other components of sensor network architecture, primarily because the sensors are limited in resources to handle memory and computation intensive methods like asymmetric cryptography. Also issues arising out of disparate ownership and cross policy domain resource access were not addressed. This effort developed a framework that incorporates authorization/authentication mechanisms that are secure and suited for disseminating and analyzing sensor information in a multi-owner environment. This effort is based on a unified architecture initially discussed at the SensorNet Architecture Forum [10] to enable the use of resources owned by disparate organizations to support the objectives of SensorNet initiative. The framework developed here contributes to the overall SensorNet initiative whose objectives are to develop technology, and indentify and promote standards and technical requirements for an integrated national warning and alert system aimed at incident discovery, awareness, and response capability. SensorNet provides a standard mechanism to move information from sensors though the Internet to end user applications. Coordination of SensorNet activities has been lead by the Oak Ridge National Laboratory (ORNL).

The main results of this effort are contained in Appendixes A-F (Table 1) and are summarized below.

| Appendix | Technical Report Number or Publication Venue | Title |
|---|---|---|
| Appendix A | ITTC-FY2008-TR-41420-03 | A Framework for Sensor Networks with Multiple Owners |
| Appendix B | Submitted to: International Conference on. Information Processing in Sensor Networks. April 22-24, 2008 | A Unified Architecture for Sensor Networks with Multiple Owners |
| Appendix C | Published in: Proc. of The Seventh IASTED International Conference on Wireless and Optical Communications, Montreal, Quebec, Canada. | A Secure Routing Protocol for SensorNet |
| Appendix D | ITTC-FY2008-TR-41420-04 | An Evaluation of Sensing Platforms Used for Sensor Network Research |
| Appendix E | Published in: Proc. of The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Oct. 9-12, 2006, Vancouver, British Columbia, Canada. | Investment Function: Enhanced Fairness and Performance in Multi-hop Wireless Networks |
| Appendix F | ITTC-FY2008-TR41420-05 | Performance Constraints of Distributed Control Loops on Linux Systems |

Table 1: Results

Appendix A contains a description of the developed architecture including the results of a prototype implementation and lessons learned.  An associated paper submitted to the International Conference on Information Processing in Sensor Networks is in Appendix B. Sensor networks are often based on resource-limited components that use wireless communication as such security challenges arise. Any attempt to secure a sensor network must balance the energy consumption and computation overhead of the scheme with the security provided. A new routing protocol that increases the resiliency of the network as well as the security of the data was developed [17] and is presented in Appendix C. Hardware platforms for sensor networks are rapidly evolving; current systems suitable for use in the developed architecture were evaluated. Appendix D contains a discussion of various platforms including capabilities, strengths and weaknesses.  This review is intended to help others in their selection of platforms for future SensorNet implementations.

Multihop wireless networks will also play a role in future sensor networks, for example, in the rail system monitoring scenario it is likely that it will be cost prohibitive to provide reach back communications for individual containers; rather a multi-hop wireless network will be used to aggregate information from several containers for reach back. A new means to enhance multi-hop fairness and efficient utilization of the scarce bandwidth in multi-hop wireless networks was developed [18] (Appendix E) where a concept, the investment function, was introduced to achieve a two-pronged objective: significant increases in network bandwidth utilization, while allocating and distributing the bandwidth among flows to promote service quality and ensure fairness among flows.

Many operational scenarios involve distributed wide area sensor networks containing one or more distributed command and control loops composed of data collection, data analysis, and actuator elements, e.g., retasking a sensor. The correctness and stability of these control loops is strongly influenced by the end-to-end communication time among its components and by the accuracy of component execution in real-time. Factors affecting the ability to achieve desired performance using open interfaces are a particularly important aspect of this task since control loop components will often have varied ownership and administrative domain membership. The distributed behavior of real-time control within such wide area sensor networks is presented here. The ability to evaluate specific instances of behavior as well as aggregate measures of longer-term behavior of distributed control loops was developed here. This form of support is required by any developer of distributed control loops.  Many components of the system software within these distributed systems can affect and constrain the overall performance of the control loop applications. Thus, determining which aspects of the system software create such constraints, and, when possible, why they are created is fundamental to effective and efficient design and implementation of such distributed control loop applications. Delay constraints imposed by supporting computational and networking components are a crucial factor in correctness of distributed control. The results described in Appendix F demonstrated that distributed control loop type computations could be implemented and their behavior evaluated in detail. The methods and tools demonstrated provide an effective platform for a wide variety of related distributed application development and evaluation.

# 2 Identification of the Potential of the Integration of SensorNet into a Rail System Monitoring Environment

A goal of this effort was also to identify new application domains to accelerate the transfer of the SensorNet technology. The basis for moving forward with a rail system monitoring environment that includes SensorNet technologies and architectures was established as part of this effort.

The motivation for focusing on the rail system arises by noting that exports from Asia to the USA, particularly Southeast Asia and China, have increased significantly over the past 10 years.  Over the past year alone, imports from China have spiked 33.2 percent and exports increased by 13.7 percent.  This large import/export volume has created a systematic limitation on key US ports, particularly the Port of Los Angeles/Long Beach, to the point where alternate west coast ports will reach full capacity in the coming years.

Conterminously, a group in Kansas City, known as Kansas City SmartPort, recognized the strategic transportation position of Kansas City and has actively worked to expand its role in domestic distribution, often as the recipient of goods originating in Asia. SmartPort is involved in several very timely and significant trade lane development projects that will result in increased traffic through the Kansas City area. Further, SmartPort is developing a US export capability and has the only Mexican Customs clearance capability that is not at the border.

This effort identified SmartPort as a potential opportunity to integrate SensorNet technology into inland port that involves multiple modes (including rail) of transport requiring a secure trade lane.

## 2.1 Background-US trade lane environment

The key ports of entry on the US West Coast are Los Angeles/Long Beach, Seattle/Tacoma, Oakland, and Portland, with LA/Long Beach dwarfing the other three. Past events on the west coast, e.g., the Longshoreman’s Strike, Union Pacific trackage problems, noise and environmental concerns, limitations of the Alameda corridor, highlight the vulnerability of that port. Further, any disaster, including terrorist attacks, will hypothetically shut down the targeted port. As a consequence, a number of companies are developing backup plans utilizing other ports. Some companies are moving their businesses to less busy ports; others are now splitting their cargos between ports. A number of companies are looking to the West-coast Mexican ports for relief. The three principal West-coast Mexican ports are Ensenada, Manzanillo, and Lazaro Cardenas. Of these, Ensenada and Manzanillo are approaching capacity. Several new ports are under construction in Baja California, and Manzanillo is beginning an expansion program. The Port of Lazaro Cardenas has been recognized as the most promising port in Mexico. Its key attributes are as follows: deepest natural port in Mexico, relatively undeveloped infrastructure, large amount of available land, rail access that does not move through urban areas, and an available stable workforce. Kansas City-based Kansas City Southern Railway, in a visionary move, acquired the largest Mexican railway, TFM, and completed that transaction in 2005. The southern terminus of TFM (which is now known as Kansas City Southern de Mexico, KCSdM) is the Port of Lazaro Cardenas. This provides the unprecedented ability to land cargo at this Mexican port and carry it on KCSdM all the way to the center of the US, i.e., terminating in Kansas City, one of the safest points of entry/departure in the United States. In a related move, Mexican Customs recognized the strategic location of Kansas City and is now building its first Customs office outside Mexico. The purpose of this office is to inspect and place in-bond cargo bound for Mexico. Kansas City SmartPort was instrumental in making this happen.

## 2.2 Developing the trusted corridor

One of SmartPort’s goals in defining its role in both international commerce and domestic distribution is the ability to offer differentiating services. SmartPort understands the reality that a natural trade corridor, running through Kansas City, exists and continues to grow. The provisions of NAFTA facilitate international trade with Mexico and Canada. Local transportation, warehousing and logistics infrastructure are capitalizing on the central location of Kansas City and are attracting other related investment. SmartPort recognizes that the changing landscape offers both opportunity and challenges. While tasked with increasing the role of Kansas City as a trade and transportation center, SmartPort also recognizes the need to effectively manage the associated risk. SmartPort has embarked on an ambitious funded project to develop the infrastructure needed to support several specific trade lanes. SmartPort has basically completed the trade lane architecture study and high level requirements. SmartPort has run limited live operational tracking and tracing tests for the planned opening of the Mexican Customs office, demonstrating cargo risk management and transportation information integration on Mexico-bound, in-bond cargo. SmartPort users have indicated the industry's need for visibility into freight and cargo movement. There are intermodal 'black holes' when freight changes hands across modes and carriers. Visibility will only be possible through the integration of carrier, shipper, broker, importer, exporter, and forwarder information. Currently, industry is demonstrating that it is possible to integrate disparate transportation information. Broader information nets needs to be set to capture the information necessary to remove 'black holes'. The natural byproducts of increased information integration are improved operations efficiencies and ultimately increased security. Information integration can be accomplished through the use of a Trade Data Exchange (TDE).

## 2.3 Trade Data Exchange

A goal of this effort was to indentify opportunities for expanding the scope of SensorNet to include inter-modal facilities specifically including a rail component. SmartPort has recognized the strategic transportation position of Kansas City and is actively working to expand Kansas City's role in domestic distribution. SmartPort, through the Mid America Regional Council (MARC), is fostering the development of several trade lane projects that will result in increased commerce in the Kansas City area. SmartPort/MARC is supporting the development of U.S. export capabilities and has the only Mexican Customs clearance capability not at the border. Specifically, SmartPort/MARC through its Intelligent Transportation Integration Project is working with EDS to develop a Trade Data Exchange (TDE) that considers inter-modal facilities to:

a. Capture commercial, clearance data, including Shipping List, Bill of Lading, Commercial Invoice, Certificate of Origin (NAFTA Letter) Shippers Export Declaration
b. Interconnect commercial, regulatory and security stakeholders
c. Validate and verify data to ensure accuracy, consistency and completeness
d. Perform forward notification to the customs broker to request verification of the trade origination documents. The customs broker accesses the TDE via the same SmartPort portal to review and verify the trade documentation
e. Monitor the progress of the documentation via the TDE and notify responsible parties when errors or incompleteness pose the threat of delaying a shipment
f. Perform risk assessment

As part of this effort a unique partnership with SmartPort/MARC and EDS was developed; also the concept integrating SensorNet information obtained via the multi-owner architecture (developed here) with the trade data exchange information was created. The TDE and the SensorNet information can be used to develop the correlation between documents and sensed environment. The result of this effort identified the opportunity as well as the potential benefits of the integration of SensorNet technologies and architectures with a TDE; also a path to testing and evaluation in a rail environment was determined.

# 3 References

[1] A. Hac. Wireless Sensor Network Designs. Wiley & Sons, West Sussex, England, 2003.

[2] D. Estrin, D. Culler, K. Pister, and G. Sukhatme. “Connecting the Physical World with Pervasive Networks”. IEEE Pervasive Computing, pp. 59–69, January-March 2002.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. “Wireless Sensor Networks: A Survey”. Computer Networks, 38:393-422, September 2002.

[4] Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culle. “Lessons from a Sensor Network Expedition”. In European Workshop on Wireless Sensor Networks (EWSN ’04), pages 66–80, Berlin, Germany, 2004.

[5] J. M. Rabaey et al., PicoRadio Supports Ad Hoc Ultra- Low Power Wireless Networking, IEEE Comp. Mag., 2000, pp. 42-48.

[6] J. M. Kahn, R. H. Katz, and K. S. J. Pister, Next Century Challenges: Mobile Networking for Smart Dust, Proc. ACM MobiCom ’99, Washington, DC, 1999, pp. 271-78.

[7] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, IEEE Proc. Hawaii Int’l. Conf. Sys. Sci., Jan. 2000, pp. 10.

[8] W. Su and I. F. Akyildiz, A Stream Enabled Routing (SER) Protocol for Sensor Networks, Medhoc- Net 2002, Sardegna, Italy, Sept. 2002.

[9] G. J. Pottie and W. J. Kaiser, Wireless Integrated Network Sensors, Commun. ACM, vol. 43, no. 5, May 2000, pp. 551-58.

[10] SensorNet Architecture Forum, August 13-14, 2003, ITTC, University of Kansas, http://www.ittc.ku.edu/workshops/sensornet/.

[11] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D.Tygar. Spins: Security protocols for sensor networks. Wireless Networks, 8:521, 534, 2002.

[12] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song, Efficient authentication and signing of multicast streams over lossy channels, In IEEE Symposium on Security and Privacy, May 2000.

[13] Bhrat Patel and Jon Crowcroft. Ticket based service access for the mobile user. In Third annual ACM/IEEE international conference on Mobile computing and networking, pages 223-233, Budapest Hungary, September 1997.

[14] David W. Carman, Peter S. Kruus, and Brian J. Matt. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report #00-010, September 2000.

[15] Secure Microcontrollers for SmartCards, www.atmel.com/atmel/acrobat/1065s.pdf.

[16] iButton: A Java-Powered Cryptographic iButton, www.ibutton.com/ibuttons/java.html.

[17] Daniel T. Fokum and Gary J. Minden, "A Secure Routing Protocol for SensorNet," Proc. of The Seventh IASTED International Conference on Wireless and Optical Communications (WOC 2007), Montreal, Quebec, Canada.

[18] Pradeepkumar Mani and David W. Petr, "Investment Function: Enhanced Fairness and Performance in Multi-hop Wireless Networks" Proc. of The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2006), Oct. 9-12, 2006, Vancouver, British Columbia, Canada.