# Towards Wireless Sensor Networks for Railway Infrastructure Monitoring

Francesco Flammini[1], Andrea Gaglione[2], Francesco Ottello[1], Alfio Pappalardo[1 2], Concetta Pragliola[1], Annarita Tedesco[1]

[1] ANSALDO STS Italy
Innovation & Competitiveness Unit
Via Argine 425, Naples, Italy
{francesco.flammini, francesco.ottello, alfio.pappalardo, concetta.pragliola, annarita.tedesco }@ansaldo-sts.com

[2] Università di Napoli Federico II
Department of Computer & Systems Engineering
Via Claudio 21, Naples, Italy
andrea.gaglione@unina.it

*Abstract*-**In recent years, there has been an increasing interest in the adoption of emerging sensing technologies for instrumentation within a variety of structural systems. Structural health monitoring systems are widely adopted to monitor the behavior of structures during forced vibration testing or natural excitation (e.g. earthquakes, winds, live loading). They can be found in a number of civil structures, including bridges and viaducts, and also in applications of vehicle health monitoring. Moreover, since infrastructures can be damaged by human originated threats, the adoption of security measures is also essential. This paper presents a proposal of an early warning system based on Wireless Sensor Networks (WSN) for railway infrastructure monitoring. It exploits already available research results and tools for WSN management, integration and data fusion. The aim is to hedge detection capabilities in a complete framework for structural failures as well as security threats, including both natural hazards and intentional attacks.**

*Keywords*-**Early warning, infrastructure protection, distributed surveillance, structural health monitoring, wireless sensor networks**

## I. INTRODUCTION

In recent years, there has been an increasing interest in the adoption of emerging sensing technologies for instrumentation within a variety of structural systems. Structural Health Monitoring (SHM) is a relatively new scientific field which aims at providing reliable data concerning the integrity of different kind of structures (fixed or mobile), in order to permit their further operational utilization or to impose their repair or retirement.

Structural monitoring systems are widely adopted to monitor the behavior of structures during forced vibration testing or natural excitation (e.g. earthquakes, winds, live loading). They can be found in a number of common civil structures among which railway bridges and viaducts.

Moreover, the very recent train bomb attack on the Nevsky Express from Moskow to St. Petersburg highlighted the attractiveness and vulnerabilities of railway transportation systems. Modern security systems used by infrastructure protection applications include a set of different sensing technologies integrated by appropriate management systems. Such systems are still highly dependent from human operators for supervision and intervention. One of the challenging goals of the research community in this field is the automatic detection of both natural and malicious threat scenarios.

This paper presents the architectural proposal of *SENSORAIL*, an early warning system based on Wireless Sensor Networks (WSNs), an emerging technology which has become a highly active research area due to their potential for providing different capabilities to a wide variety of applications [1]. Wireless sensors and sensor networks technologies have begun to be considered as substitutes of traditional tethered monitoring systems in structural engineering and critical infrastructure surveillance fields [1, 3, 4, 16]. WSNs enable dense monitoring of large physical structures and promise enormous ease and flexibility of deployment of instrumentation (extensive wiring is no longer required between sensors and the data acquisition system), as well as low maintenance and deployment and instrumentation costs. Due in part to the complexity of such systems, developing sensing applications on a network of wireless sensors remains a difficult and time-consuming endeavor. However different middleware platforms have been proposed for WSNs, which refers to software and tools providing a system abstraction so that the application programmer can focus on the application logic without having to deal with lower level implementation details [5].

SENSORAIL exploits already available research results, frameworks and tools for the integration of heterogeneous sensors with the aim of continuously and automatically checking environmental parameters to provide an early warning system for structural failures and security threats, including both natural hazards and intentional attacks. The system uses clusters of sensors which interconnected by WSN

978-1-4244-9094-3/10/$26.00 ©2010 IEEE

and can communicate events to remote control centers using GSM-R/GPRS mobile terminals.

We have already developed two frameworks allowing for the integration of different and heterogeneous sensor networks (SeNsIM [6]) and the detection of events of any complexity by a model-based data correlation (DETECT [7]). As for SHM, we exploited the Tenet system, an architecture for tiered sensor networks, which has been preliminary experimented for rail bridge monitoring [8, 14].

SENSORAIL is a project carried out by the Innovation Unit of Ansaldo STS Italy and covering the growing markets of structural health monitoring and infrastructure security. It is expected to be an attractive product for potential customers due to its originality, cost-effectiveness, easy installation and maintenance. All these factors contribute to keep low the time-to-market as well as the acquisition and operational costs for the customers. Furthermore, it can be installed also where there is no power source or wired telecommunication facilities (which is rather frequent on railway lines), since the system can be powered by batteries and/or solar cells and it exploits wireless transmission for both sensor-to-sensor and sensor-to-control center communications.

## II. RELATED WORKS

Presently, conventional methods for SHM systems employ coaxial wires for communication between sensors (i.e. piezoelectric accelerometers) and a central PC-class device. While coaxial wires provide a very reliable communication link, they are time consuming to install and quite expensive. For example a piezoelectric acceleration sensor for modal analysis costs about 3000€ to 5000€ and data acquisition and cabling for each sensor costs about 1000€ to 2000€. Therefore, in recent years many research efforts have been devoted to the development of Optical Fiber Bragg Grating (OFBG), Polyvinylidene Fluoride (PVDF), Carbon Fiber-Reinforced Polymer (CFRP) sensors [9, 10]. Although these kinds of sensors can provide high-resolution measurement capabilities that are not feasible with conventional techniques they are very expensive and need to make a great effort to research and develop.

The essence of structural health monitoring (SHM) requires an innovative sensing system similar to a human nervous system throughout the whole body to catch comprehensive information without losing structural integrity.

The durability of sensors themselves is one of key problems. Although the optical fiber sensors possesses evident advantages compared with other structural local performance sensors, sensors to monitor the durability of structural members, such as steel corrosion, concrete carbonization etc, need to make a great effort to research and develop.

Ubiquitous wireless networking calls for efficient dynamic spectrum allocation (DSA) among heterogeneous users with several transmission types and bandwidth demands. In fact, in order to meet typical critical requirements for a strategic infrastructure, such as the user-specific quality-of-service (QoS), the power and spectrum allocated to each user should lie inside a bounded region to be meaningful for the intended application. This requires high bandwidth availability and certainly beyond the large number of distributed sensors

Moreover, an infrastructure for SHM often includes several hundreds or even several thousands of sensors; the transmission line of sensing signals is one of key factors influencing the properties of sensors and system reliability.

In Table 1 we show a comparison between traditional and wireless sensor network focused on the most important network characteristics.

TABLE I
COMPARISON BETWEEN TRADITIONAL AND WIRELESS SENSOR NETWORK

| Characteristics | Traditional SN | Wireless SN |
|---|---|---|
| sensors number | few | many (smart dust) |
| node accuracy | high | low |
| node reliability | high | low (prone to failure) |
| node redundancy | low | high |
| node resources | high | low |
| node cost | high | low |
| processing | centralized | distributed, hybrid |
| transmitted data | raw | processed |
| transmission accuracy | high | low |
| transmission reliability | high | low |
| transmission range | high | low |
| transmission BW | high | low |
| network topology | fixed | may change frequently |
| network organization | very simple | functional clusters |
| uncertainty | close to minimum | lifetime tradeoff |

In many applications, wireless sensor networks can improve the human abilities of perception and control. Relevant examples are home automation (HVAC, Lighting, Remote door openers, Security and Smoke Detectors, Smart Appliances), Industrial and Commercial Building Monitoring (Security and Surveillance, Smart Energy, Process Control, Structural Health Monitoring, Seismic monitoring), human health monitoring (Wearable Sensors, Emergency Response, Elderly Care), automotive (Tire Pressure monitoring, Remote Keyless Entry, Hands-free command units, Engine Control, Traffic Management, Transportation Safety). In particular, as for lineside security monitoring, though considered a need by the operators, it is rarely performed in railway systems due to the length of the lines and the difficulties in providing power supplies and telecommunication facilities in an affordable way.

As mentioned above, conventional monitoring systems consisting of a larger amount of sensors are high-priced expensive and therefore can only be installed on a few sites of a physical infrastructure, above all if the latter is quite extended. Hence, Wireless Sensor Networks could reduce these costs dramatically. Several Wireless Sensor Networks systems have been proposed for SHM [8, 11, 12]. The basic principle lies in an architecture able to collect data locally on a specific point of the infrastructure and send relevant data (alarms) to a control center for offline analysis. The authors of BriMon [17] have designed a novel event detection mechanism that triggers data collection in response to an oncoming train, in order to save sensor energy when it is not required a continuous monitoring of the infrastructure. In [18], a wireless sensor networking architecture to monitor the health of railway wagons attached to a moving locomotive is presented. The aim is to develop a vehicle monitoring system to reduce the maintenance and inspection requirements of railway systems whule maintaining safety and reliability.

In the aim of an EU Brite-EuRam funded project entitled MILLENNIUM—''Monitoring of Large Civil Engineering Structures for Improved Maintenance'' two fiber optic-based monitoring systems have been designed, developed, and tested with laboratory and field trial environments [13].

The field trial was undertaken on the Mjosundet BridgeThis bridge is located in Aure, about 50 km north of Kristiansund on the west coast of Norway. It is a five-span continuous composite bridge. The optical fiber sensors were mounted inside the bridge in conjunction with conventional strain gauges.

The results lied that, besides showing that the accuracy of FOSs mounted in real structures is as good as for traditional sensors, the long-term performance of such sensors and the possibility of sensor trees to be easily manufactured up to thousands of meters in length, makes them ideal for large-scale continuous monitoring in civil engineering structures. Similar objectives are not affordable for traditional electrical-based techniques.

## III. THE SENSORAIL APPROACH TO INFRASTRUCTURE MONITORING

The aim of SENSORAIL is to perform an extensive monitoring of (part of) a railway system against the most common threats. As already mentioned, it is suitable for two main applications (both regarding rail transportation systems): structural health monitoring, especially for critical assets, and environmental security monitoring, that is fire, explosions, earthquakes, floods and landslides detection along the track. The system can be extended by integrating sensors of different nature to provide other supervisory functionalities. For instance, on-board sensors could be added to monitor freight train integrity and continuously transmit these data in real-time to ground devices and thus to the security control center; such an application could take the advantage of the alternative powering possibilities of WSN, since many freight cars do not feature any power supply. Another possible application is the fence vibration detection for perimeter intrusion detection on track lines or inside train depots. Generally speaking, both the hardware and the middleware can be reused to fit any monitoring application, including environmental surveillance of the internal of passenger cars for comfort or abnormal events like high temperature, out of range vibrations, high intensity noises (possibly indicating screams, gunshots or explosions).

The core of our overall architecture is the SeNsIM (Sensor Networks Integration and Management) [6] framework, which is an integration platform for heterogeneous sensor networks. Different kind of sensor systems can be adopted for the protection of railway infrastructures (i.e. temperature sensors, NBCR sensors, intelligent videocameras, etc.). SeNsIM provides a generic user with a unique way to manage, query and interact with such systems and solves heterogeneity issues in data representation of and data retrieval from different networks.

In order to recognize security threats against the railway infrastructure we use the DETECT system, a reasoning module which operates by performing a model-based correlation of events retrieved by sensor systems and trying to detect or, if possible, prevent threats against the physical infrastructure.

As for SHM, we use the Tenet system, integrated in the SeNsIM framework. Tenet is an alternative architecture for tiered sensor networks which allows an easy deployment of data retrieval tasks on such systems. In [14], an interesting proposal on how to use Tenet for Structural Health Monitoring applications is shown.

### *A. The SeNsIM platform*

SeNsIM is an integration platform for heterogeneous sensor systems/networks. It is not just a middleware for sensor networks, but a more general software architecture which makes possible the deployment of applications based on multiple sensor systems/networks and allows a generic user or an application to easily access data sensed by a network.

SeNsIM provides a unique interface for local networks that allow a generic user to express queries by means of an intuitive query visual language. It was conceived with the aim to bridge the gap between heterogeneous sensor systems and to provide a generic user/application with a unique way to manage, query and interact with them. Nowadays there is a tremendous heterogeneity in the logic for interfacing and collecting data from sensor systems. The major issue of an integrating system lies in the heterogeneity of the hardware to sense data and of the repositories, these make data management and retrieval processes hard tasks to achieve.

Furthermore, sensor data may be differently structured according to the specific representation of different sensor systems. In order to face such problems SeNsIM defines:

- an *architectural model* able to support in an efficient way the management of data even when sensed by different networks;
- a *data model* capable of representing in a unique format both sensor data and sensor systems.

SeNsIM architectural model has been designed by exploiting the *wrapper-mediator* paradigm, a well-known technique to integrate data from heterogeneous source [15], in which the *mediator* component accesses different data sources by means of ad hoc connectors (*wrappers*). In SeNsIM, each wrapper explores and monitors the local sensor network and sends to the mediator an appropriate description of the related information according to the common data model. On the other hand the mediator organizes such information and keeps a unique view of all systems in order to satisfy user or application queries.

Such a scenario is quite realistic in the context of railway infrastructures where different kind of sensor systems can be adopted for their protection (i.e. temperature sensors, NBCR sensors, intelligent videocameras, etc.). The reference architecture of the SeNsIM framework is shown in Figure 1.

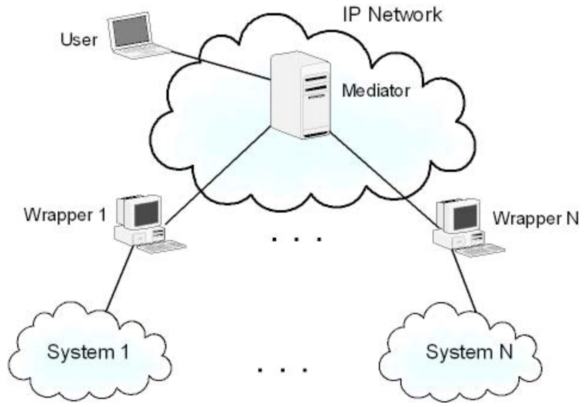


Fig. 1. SeNsIM architecture

### B. The DETECT framework

The basic assumption behind the DETECT framework is that threats can be detected by predicting the set of basic events (i.e. the patterns) which constitute their "signature". Threat scenarios must be precisely identified during Vulnerability Assessment and Risk Analysis. DETECT operates by performing a model-based logical, spatial and temporal correlation of basic events detected by different sensor subsystems, in order to recognize sequence of events which indicate the likelihood of threats. DETECT is based on a real-time detection engine which implements the concepts of data fusion and cognitive reasoning by means of soft computing approaches. The framework can be interfaced with or integrated in existing SMS (Security Management Software). It can serve as an early warning tool or even to automatically trigger adequate countermeasures for emergency/crisis management.

As such, it may allow for a quick, focused and automatic response to emergencies, though manual confirmation of detected alarms remains an option. In fact, human management of critical situations, possibly involving many simultaneous events, is a very delicate task, which can be error prone as well as subject to forced inhibition. Used as a warning system, it can alert the operators about the likelihood and nature of the threat; used as an autonomous reasoning engine, it can activate responsive actions, including audio and visual alarms, unblock of turnstiles, air conditioned flow inversion, activation of sprinkles, emergency calls to first responders, etc. Furthermore, the correlation among basic events detected by diverse redundant sensors can also be employed to lower the false alarm rate of the security system, thus improving the overall reliability of the security system.

Threats are described in DETECT using a specific *Event Description Language* (EDL) and stored in a *Scenario Repository*. Starting from the Scenario Repository, one or more detection models are automatically generated using a suitable formalism (e.g. Event Graphs, Bayesian Networks, Neural Networks, etc.). In the operational phase, a model manager macro-module has the responsibility of performing queries on the Event History database for the real-time feeding of detection model according to predetermined policies. When a composite event is recognized, the output of DETECT consists of: the identifier(s) of the detected/suspected scenario(s); an alarm level, associated to scenario evolution (used as a progress indicator); a likelihood of attack, expressed in terms of probability (used as a threshold in heuristic detection). A high level architecture of the framework is depicted in Figure 2.

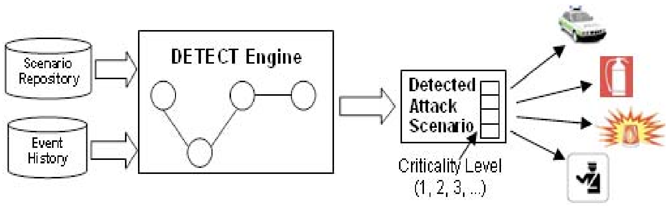


Fig. 2. The DETECT framework

## IV. A POSSIBLE REFERENCE ARCHITECTURE

SENSORAIL can be advantageously integrated with existing security surveillance systems sharing the same hardware (at the distributed sensors level) and sensor integration middleware (i.e. SeNsIM), using either:

- dedicated software for structural health monitoring (e.g. Tenet) running as a stand-alone data fusion application;
- natural hazard scenario descriptions in EDL added to DETECT threat repository.

For instance, EDL descriptions operating at the decision fusion level can be based on already defined sensor-level abnormal conditions to correlate multiple alarms in order to improve detection reliability (e.g. abnormal event detected by at least K sensors) or even on more complex scenarios (e.g. vibration sequence on bridge sensors which is different from the one generated by the normal passage of the train). Please note that the two approaches are not mutually exclusive.

Regardless of how the software system is implemented, Figure 3 shows a possible overall hardware architecture of SENSORAIL. Distributed smart-sensors are installed along

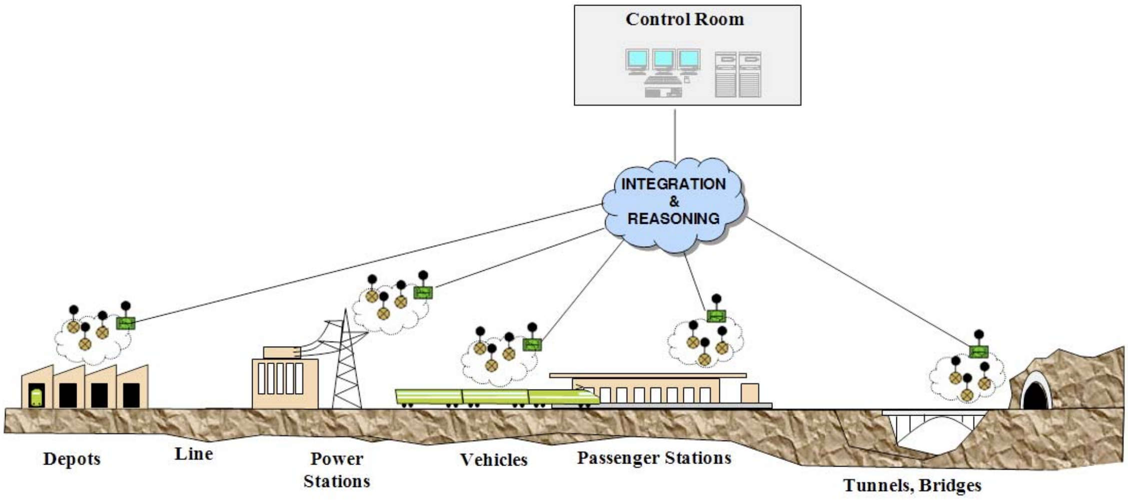


Fig. 3. SENSORAIL architecture

the railway line both in fixed (e.g. bridges, tunnels, stations, etc.) and mobile (passenger trains, freight cars, etc.) locations. They are integrated locally using local wireless infrastructures (e.g. Wi-Fi, ZigBee, etc.) and then data is collected by WSN gateway nodes and transmitted remotely by means of WAN (Wide Area Network) infrastructures, like:

- GSM/GPRS, providing communication bandwidth (few hundreds Kb/s) enough to transmit life signals, alarm messages and possibly camera screenshots, whenever available;
- UMTS/EDGE or Satellite links (few Mb/s bandwidth), which can additionally transmit a few video-streams from neighbour cameras in case of abnormal event detection by sensors, in order for the operators to verify alarms in real-time (the actual video quality and frame-rate depending on how many cameras are involved);
- Fiber Optics geographic networks along the line (only possible for fixed sites), which provide a very high bandwidth (in the Gb/s range), also allowing to transmit high-resolution videos at very high frame-rates (e.g. 25 FPS) for a superior situational awareness at the control rooms.

In conclusion, low/average bandwidth networks are strictly required to transmit alarms to the control center, which are often already available (like GSM-R for railways) or easy to deploy (like satellite) and provide an extensive coverage of the infrastructure. However, if high-quality video streams from cameras need to be shown to the operators in order to verify the alarm and/or supervise the situation, higher bandwidth is required which can be possible achieved by multiple low bandwidth connections.

## V. An Example Application: Freight Train Monitoring

Currently there are still a few proposals for the vehicles monitoring in order to ensure a safe & secure operation of the transportation system. The detection of abnormal operating or environmental conditions on board of vehicles as well as threats of burglary represents an example application of great interest for the freight train monitoring.

The use of a sensors network consisting of wireless nodes, allows for more flexibility in the installation, both in terms of deployment of the nodes and global coverage of the vehicle (independent of availability of cables in certain areas and their length). This aspect represents a significant advantage in the considered context and allows for exploiting also the redundancy of the sensors (if any) in order to make the network more robust and reliable.

In Figure 4 we provide a scheme for the remote monitoring of unpowered freight cars possibly used to transport valuable and/or hazardous materials, based on the following devices:

- A: Access control device powered on-demand (e.g. numeric keypad featuring “ON” button);
- B: Long lasting battery pack;
- C: Magnetic contact or other very-low consumption intrusion detection device;
- F: FPGA-based central control unit featuring embedded CPU and OS;
- G: Low size power generator (e.g. eolic, solar panel, piezoelectric pad) – optional;
- M: Self-powered smart wireless sensor measuring vibrations, temperature, humidity, light, sound;
- N: Gateway node for the wireless sensor network;
- S: Satellite positioning antenna;
- T: Wide area wireless transceiver (GSM, GPRS, UMTS, EDGE).

The basic working logic of the system is as follows.

- Case of abnormal environmental or operational conditions: whenever an abnormal event (e.g. very high temperature or out of range vibrations) is detected by M, its transmission unit is activated and data is received by N. F validates data and - if the anomaly is confirmed - it activates S to achieve the current position and T to send an appropriate warning message to the control center.

- Case of intrusions: whenever C detects an opening while the alarm system is activated (by A), F activates S to achieve the current position and T to send an appropriate alarm message to the control center.

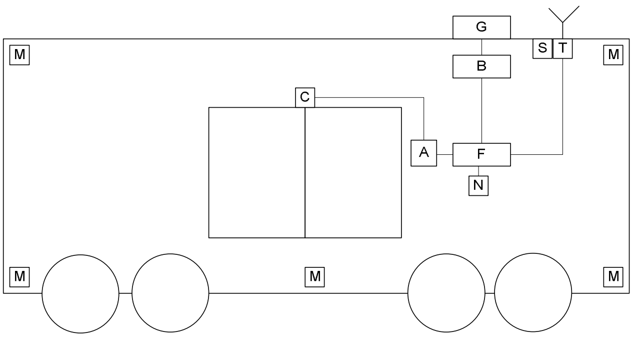


Fig. 4. Integrated monitoring system for freight cars

## VI. CONCLUSIONS

We have presented the architectural proposal of SENSORAIL, an early warning system suitable for both structural health monitoring and infrastructure surveillance against natural hazards and intentional threats. It exploits available research results and tools in the field of sensor networks integration, WSNs for SHM and threat detection. The idea is at the experimentation stage, with the aim to be integrated in security management systems already developed by Ansaldo STS.

The use of wireless sensors for SHM is a cost-effective solution, since the devices are cheap, auto-configuring and thus easy to install and substitute. They can also be installed where there is no power source or wired telecommunication facilities (which is rather frequent on railway lines), since they are powered by batteries and/or solar cells and exploit wireless transmission for both sensor-to-sensor and sensor-to-control center communications.

## REFERENCES


[1] I. F. Akyildiz, M. C. Vuran, O. B. Akan, W. Su, "Wireless Sensor Network: A survey REVISITED," in *Computer Networks Journal*, 2005.

[2] R. Roman, C. Alcaraz, and J. Lopez, "The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection," in *Inf. Secur. Tech. Rep.*, Vol. 12, No. 1, pp. 24-31, January 2007.

[3] J.P. Lynch, K.J. Loh, "A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring," in *The Shock and Vibration Digest*, pp. 38-91, 2006

[4] F. Flammini, A. Gaglione, N. Mazzocca, V. Moscato, C. Pragliola, "Wireless Sensor Data Fusion for Critical Infrastructure Security," in *Proc. International Workshop on Computational Intelligence in Security for Information Systems CISIS'08 - Advances in Soft Computing*, pp. 92-99, 2008.

[5] S. Hadim, N. Mohamed, "Middleware for wireless sensor networks: A survey," in *Proc. 1st Int. Conf. Comm. System Software and Middleware (Comsware06)*, New Delhi, India, Jan. 8-12, 2006.

[6] V. Casola, A. Gaglione, A. Mazzeo, "A Reference Architecture for Sensor Networks Integration and Management," in *Proc. Third International Conference on Geosensor Networks* (Oxford, United Kingdom, July 13-14 2009), LNCS, vol. 5659, Springer-Verlag, Berlin, Heidelberg, pp.158-168, 2009.

[7] F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola, "DETECT: a novel framework for the detection of attacks to critical infrastructure," in *Safety, Reliability and Risk Analysis: Theory, Methods and Applications* - Martorell et al. (eds), Proc. ESREL'08, pp.105-112, Valencia, Spain, September 22-25 2008, pp. 105-112 (CRC Press, Taylor & Francis Group), London, 2008.

[8] J. Paek, B. Greenstein, O. Gnawali, K.Y. Jang, A. Joki, M. Vieira, J. Hicks, D. Estrin, R. Govindan, E. Kohler, "The Tenet Architecture for Tiered Sensor Networks," in *ACM Transactions on Sensor Networks (TOSN)*, Vol. 6, No. 4, 2010.

[9] J. Ou, H. Li, "Recent Advances of Structural Health Monitoring in Mainland China," in *Proc. ANCER Annual Meeting*, Hawaii, July 2004.

[10] S. Li, Z. Wu, "Development of Distributed Long-gage Fiber Optic Sensing System for Structural Health Monitoring," in *Structural Health Monitoring*, Vol.6: 133-143, 2007.

[11] N. Xu, S. Rangwala, K.K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, D. Estrin, "A wireless sensor network for structural monitoring," in *Proc. 2nd international conference on Embedded networked sensor systems (SenSys '04)*, Baltimore, MD, USA, 2004.

[12] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, M. Turon, "Wireless sensor networks for structural health monitoring," in *Proc. 4th international conference on Embedded networked sensor systems (SenSys '06)*, Boulder, CO, USA, 2006.

[13] Joan R. Casas and Paulo J. S. Cruz, "Fiber Optic Sensors for Bridge Monitoring," in *Journal of Bridge Engineering*, Vol. 8, Issue 6, pp.362-373, December 2003.

[14] J. Paek, O. Gnawali, K.-Y Jang, D. Nishimura, R. Govindan, J. Caffrey, M. Wahbeh, S. Masri, "A Programmable Wireless Sensing System for Structural Monitoring," in *4th World Conference on Structural Control and Monitoring (4WCSCM)*, San Diego, CA, July 2006.

[15] G. Wiederhold, "Mediators in the architecture of future information systems", in *IEEE Computer*, Vol. 25, N. 3, 1992.

[16] M. Cinque, D. Cotroneo, G. De Caro, M. Pelella, "Reliability Requirements Of Wireless Sensor Networks For Dynamic Structural Monitoring," in *Proc. International Workshop on Applied Software Reliability (WASR 2006)*, Philadelphia, USA, June 2006.

[17] K. Chebrolu, B. Raman, N. Mishra, P.K. Valiveti, R. Kumar. BriMon, "A Sensor Network System for Railway Bridge Monitoring," in *Proc. 6th International Conference on Mobile Systems, Applications, and Services (ACM MobiSys'08)*, Breckenridge, CO, June 2008.

[18] G.M. Shafiullah, A. Gyasi-Agyei, P. Wolfs, "Survey of Wireless Communications Applications in the Railway Industry," in *Proc. 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, Sydney, Australia, August, 2007.