SECURING FREIGHT TRAINS FOR HAZARDOUS MATERIAL TRANSPORTATION: A WSN-BASED MONITORING SYSTEM

Valentina Casola[(a)], Alessandra De Benedictis[(a)], Annarita Drago[(a) (b)], Mariana Esposito[(a) (b)], Francesco Flammini[(b)], Nicola Mazzocca[(a)]

[(a)] Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II
Via Claudio 21, Napoli, Italy

[(b)]Ansaldo STS
Via Argine 425, Napoli, Italy

[(a)]{casolav, alessandra.debenedictis, annarita.drago, mariana.esposito, nicola.mazzocca}@unina.it

[(b)] francesco.flammini@ansaldo-sts.com

ABSTRACT

In recent years the interest in monitoring infrastructures has spread in many application domains, even because of the number of natural disasters and terrorist attacks. This important activity can be seen in the general context of critical infrastructure protection such as the freight train meant for hazardous materials transportation. The design of these systems must answer to several issues: low-cost, easiness of installation, interoperability of information sources, security mechanisms. The use of wireless sensor networks emerged in this field as a compliant solution to these issues. In this paper we will present a monitoring system that uses heterogeneous WSN to monitor a freight train transporting hazardous materials. The sensors interact through a security platform in order to share different information. We illustrate some details on the architecture and the software application to prove the feasibility of such system on a real scenario by discussing most significant results about measurement parameters and networks performance.

Keywords: Wireless Sensor Networks, Security protocols, Data Integrity, Train protection.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in several critical application domains, as environmental monitoring, detection and classification of objects in military and civil settings, critical infrastructure monitoring and protection, automotive, health monitoring and so on. They can be easily deployed in harsh environments and do not need a supporting infrastructure, thus enabling unattended operations. A typical monitoring system is made of different sensor networks that can be heterogeneous in the technology aspects, in the data formats, in synchronization and localization standards, but also in security mechanisms. They can be connected in different ways and their data should be elaborated by the same application to enrich the knowledge of observed complex phenomena.

Among different critical infrastructures, railway and transportation infrastructures have gone through rapid developments in the last two decades, in several technological aspects including their communication systems. In the past, wired communication systems were used for signalling and data communication in the railway industry, while recently wireless communication systems have emerged as alternatives to substitute wired systems (Lynch and Loh 2006; Li and Wu 2007; Joan, Casas and Cruz 2003; Chebroul, Raman Mishra, Valiveti and Kumar 2008). Wireless systems can be used to monitor and protect critical assets within a railway infrastructure, in order to ensure reliable, safe and secure operations but also to protect citizens from any natural or anthropological hazards (Flammini, Gaglione, Ottello, Pappalardo, Pragliola and Tedesco 2010). New monitoring systems are available in the literature, they are tipically tailored for specific domains and specific technologies, they are not cost-less customizable for new scenarios and they do not easily integrate new technologies or different data models. Furthermore, they usually do not provide any mechanisms to meet security requirements as data integrity and confidentiality that are primary requirements for any critical application domains. We designed a monitoring application based on wireless sensor networks that primary copes with two different aspects: (i) interoperability of different sensor networks (in terms of technologies and security mechanisms), (ii) enforcement of different security mechanisms to provide confidentiality, authentication and integrity of exchanged messages. Within the pShield project (Artemis 2011; Casola, Esposito, Flammini and Mazzocca 2012), we had the opportunity to verify the application and the feasibility of a WSN deployment in a real scenario to protect a freight train. In fact, we installed a WSN on a train available in the Roma Smistamento station and tested our monitoring system. In this paper we will illustrate the architecture of the monitoring system and application by illustrating the main interoperability and security issues we were able to face and, finally, we will illustrate the case study by discussing some experimental results gathered in a real scenario. The remainder of this paper is structured as follows: In Section 2 we will present the motivations and open issues that are behind the choice of adopting Wireless Sensor Network in monitoring transportation infrastructures. In Section 3 we will illustrate a monitoring system that is able to integrate different sensor networks with different security requirements. In Section 4 we will illustrate the results of the experimentation and finally, in Section 5, some conclusions and future work will be drawn.

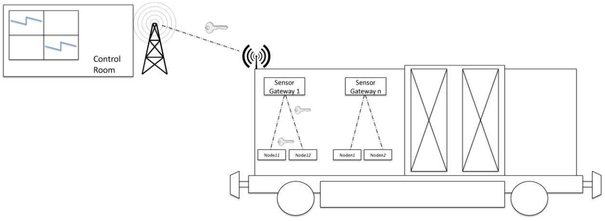

Figure 1: The System View

2. MOTIVATION

In recent years the transport by rail of dangerous goods has increased substantially and consequently the problem of their control and monitoring has became of utmost importance especially if we consider the negative effects and damages that can be caused to people and environment by any accident.

In this regard, the measurement of parameters as acceleration, vibration and position of the wagon could be used to establish if a vehicle is properly moving while temperature and humidity measurement can help to monitor and ensure optimal conditions for the transported goods and/or to prevent the risk of fire. Furthermore, with the adoption of localization tools, as a GPS receiver, it is possible to associate a set of coordinates to an event and send this information for alarm data quality improvement.

Very often, these parameters are measured by sensors already available and deployed, sometimes by new or just installed sensors, both can contribute to the observation of phenomena but there is the need to collect and manage data coming from different and heterogeneous sensor technologies. Indeed, a monitoring infrastructure is a complex system composed of several components, distributed in different points of the infrastructure to protect (e.g. on board train and on the ground) that have to communicate each other to gather the information and properly elaborate them.

In the case of rail domain there are some available solutions, they make use of standard solutions for complex distributed systems and wired sensors available on the wagons, however, in the case of freight trains, there are additional constraints. Indeed, the majority of freight cars are, currently, unpowered hence the need for a power-autonomous system. Furthermore, the railway infrastructures are geographically distributed and some components are mobile, too.

Wireless Sensor Networks (WSN) can be successfully used for such monitoring purposes. In particular, tiny sensors measure different parameters and send results to the gateway, periodically or on demand. The gateway forwards the results to a control center for a further processing and analysis according to a specific application.

In figure 1 the main components that should be deployed to monitor a freight train are illustrated. In particular, we designed different heterogeneous networks deployed inside the car to monitor different parameters with different technologies. They send the retrieved data to a centralized control Room, this collects data and elaborate them according to a specific target application.

The wireless communications for data exchange (both within the sensor networks and between the gateway and control room) should protect data from not authorized access and from other kind of attacks whose aim is to corrupt data integrity.

According to this scenario, we focused our attention on heterogeneity and security issues to design a monitoring system based on wireless sensor networks; unfortunately the solutions for securing data and manage the heterogeneity of data format and syntax available in traditional distributed systems, are not useful in wireless sensor networks because of their resource (CPU, memory, protocols,...) and power constraints.

In the following sections we are going to discuss in details such constraints and open issues, we developed a monitoring system and we deployed it in a real scenario to verify the feasibility of the proposed approach.

2.1. Heterogeneity and security issues

The wide range of parameters to observe (e.g. temperature, humidity, acceleration, GPS coordinates...) could require the deployment of several networks on the car. Such networks could be either legacy and already available or new, each having their proper hardware and software characteristics.

Distributed applications require to collect information from different sources, retrieved data are usually heterogeneous from many points of view (data structure, data format, semantic, protocols, sensing technologies) and they need to be integrated to share the common monitoring objective. Different middleware platforms based on macroprogramming models have been proposed (Hadim and Mohamed 2006; Henricksen and Robinson 2006; Romer 2004; Amato, Casola, Gaglione and Mazzeo 2011) in order to bridge the gap between the application and the underlying hardware and network platforms.

It is plain that security plays a fundamental role in the development of monitoring applications. Data collected by sensors from the environment are sensitive and they should be accessed only by authorized users since a malicious user could attack the network sending corrupted data and compromising the monitoring activity.

Several attacks against WSNs exist and can performed in many ways and at different level (Wood and Stankovic 2002). The communication among sensors is performed via a radio channel which is insecure by nature then this makes a WSN vulnerable to many attacks. Moreover, due to the resource limitation (in terms of energy, memory, computation and communication capabilities) protocols and algorithms proposed for traditional ad hoc networks are not suitable to small sensors (Ravi, Raghunathan and Kocher 2004). Furthermore in most cases, nodes are easily accessible, they can be reprogrammed, replaced or even destroyed. To achieve this goal the WSN must be designed to comply with security requirements such as authentication, integrity and confidentiality; for these reasons new approaches that try to balance security, performance and power consumption are investigated.

The fulfillment of requirements can be achieved primarily by using the cryptography but, due to discussed constraints, not all available schema are applicable: in the Symmetric Key Cryptography (SKC) a unique secret key is used to encrypt and decrypt data, while in Public Key Cryptography (PKC) a pair of keys is used one for each operation.

Until a few years ago the less resource-consuming symmetric schemes were adopted. This choice was dictated by the impossibility to use asymmetric ones (i.e. RSA) (Rivest, Shamir andAdleman 1978) as they are power consuming and require a large amount of computational and storage resources. Recent studies have shown that it is possible to implement PKC to sensor networks by exploiting the primitives offered by the Elliptic Curve Cryptography (ECC) (Kapoor, Sonny and Singh 2008). The strength of this schema is to offer equal security with smaller keys and simpler computations, thereby reducing processing and communication overhead. For example, ECC with 160 bits key provides the same security level compared to RSA with 1024 bits. Some open issues is related to the initial phase of these protocols when the nodes should agree on common secrets to initialize the security mechanisms. We investigated the adoption of different security mechanisms within the WSN, proposed hybrid approaches to cope with open problems and evaluated them from different perspectives (Casola, De Benedictis, Mazzeo and Mazzocca 2011). Among the other heterogeneous features, the monitoring application has to take into account that different networks can enforce different security mechanisms, too.

3. SENSIM-SEC FOR THE PROTECTION OF RAILWAYS

To face interoperability and security issues, we can consider a monitoring infrastructure as composed of two main layers: the sensor network layer and a distributed application layer for the management and elaboration of queries and data. In some previous papers, we introduced SeNsIM-SEC (Casola, Gaglione and Mazzeo 2009; Casola De Benedictis, Mazzeo and Mazzocca 2011), a framework based on a wrapper-mediator paradigm that was designed for integration of heterogeneous sensor networks able to manage the heterogeneity not only in the technology aspects but also in the different security requirements (see Figure 2).

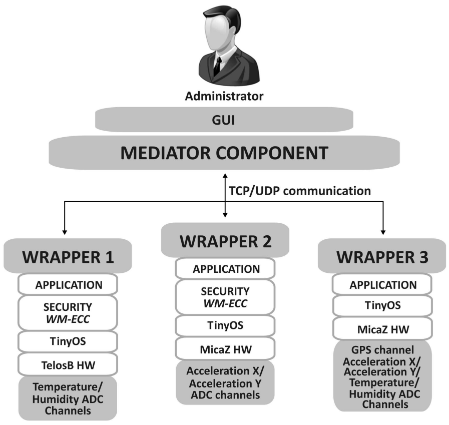

Figure 2: The SeNsIM-SEC architecture for a train

To face interoperability issues, in SeNsIM-SEC, each different network is managed by a dedicated wrapper. It communicates with the specific underlying technology and acts as a connector for the mediator component. The mediator is responsible to properly format user requests and forward them to the different wrappers. Each wrapper translates the incoming queries and forwards them into the underlying networks, retrieves the results and passes them back to the mediator. The communication between the mediator and wrappers is carried out by means of XML files, written according to a standard format and containing information about the structure of the underlying networks, the user-defined query parameters and the retrieved results.

As illustrated in figure 2, the developed architecture for train monitoring is composed of a mediator component, accessible by an end-user via a GUI interface, and of three different wrappers, each managing a different WSN, each of them has specific sensors on board as illustrated in the next section.

When application starts the mediator listens for incoming connections, which will arrive on a UDP Socket bound to a specific port (this information, along with the IP address of the mediator machine is specified in a configuration file which is read by the wrapper component at its startup). When receiving a connection request, the mediator chooses a free port and sends it to the wrapper in a datagram packet . The wrapper uses such port as the remote TCP port to send, via a TCP communication, a struct.xml file containing the specification of the connected network. Each sensor network is composed by two kind of nodes:

1. the master node is responsible of forwarding the queries coming from the wrapper by the UART interface to other nodes, and to send back the result samples;
2. the mote node starts the sensing when they receive a query.

In figure 3 is represented a network example: the node with ID=0 acts as a master and it is directly connected to the Wrapper via a serial interface, it manages the query towards the other nodes of the same network; in this example the mote nodes with ID 4 and 5 are connected via a radio channel to the master and execute the queries by sampling temperature and humidity values.

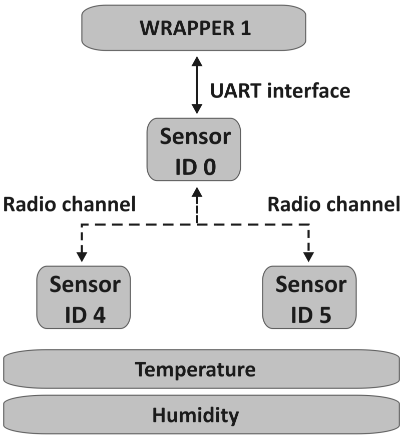

Figure 3: An example of sensor network connection

3.1. Security protocols

To secure the sensor network, security mechanisms were introduced to fulfill nodes authentication, data confidentiality and integrity requirements. These goals were achieved through the use of key exchange agreements, digital signature protocols and data encryption operations, partially provided by the WMECC library (Wang, Sheng, Tan and Qun Li 2007) that implements Elliptic Curve Cryptography (ECC).

WM-ECC is a public available open source implementation of a 160-bit ECC cryptosystem targeted to MICAz, TelosB and Tmote Sky platforms, based on recommended 160-bit SECG (Standards for Efficient Cryptography Group) elliptic curve parameters. The WM-ECC library provides all the ECC operations and some of them are optimized to give the best possible performance; it also provides an implementation of ECDSA (Elliptic Curve Digital Signature Algorithm) protocol but it does not support any key exchange protocol. We aided the application running on nodes with an implementation of the ECDH (Elliptic Curve Diffie Hellman) protocol that allows to establish a unique secret shared key that is used as a symmetric key between the master and the motes for encrypting and decrypting the messages. The encryption and decryption operations are performed by means of the Skipjack cipher, with 80 bit keys and 64 bit blocks.

Figure 4 illustrates the secure communication protocol, putting in evidence the three needed phases:

1. ECDH phase. In the first phase the master and mote nodes exchange their public points to calculate the shared secret key through the primitives provided by ECDH protocol.
2. ECDSA phase. At the arrival of a query, the master node constructs a query message with the received parameters, digitally signs it and then broadcasts it to the mote via radio channel; when receiving a query message, the mote verifies the digital signature and starts the sampling of the required physical values, according to the query parameters, only if the verify procedure is successful, otherwise it discards the message.
3. Encrypt/Decrypt phase. When the results are ready, the mote inserts them into the payload of the response message, which is encrypted with the shared key obtained in the ECDH phase and finally it sends the message to the master; at the arrival of the message, the last extracts the payload, decrypt it with shared key obtained at the first phase and then returns the query results.

We implemented this protocol for securing the communication of all nodes in the networks.

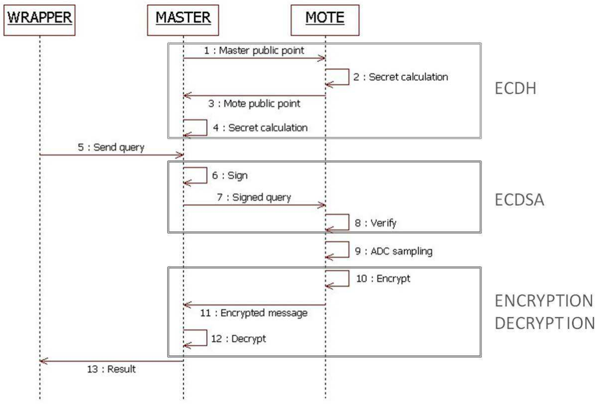

Figure 4: Secure communication protocol

4. THE EXPERIMENTAL CASE STUDY

The SeNsiM-SEC platform was installalled on a freight car made available by the Italian Railway Authority (RFI/Trenitalia) at Roma Smistamento. In figure 5, is showed the car used for the experimentation.

Figure 5: The car outside and inside

The control room was at 30 meters from the stationary train position. As illustrated in Figure 6, on the cars there are 8 sensors, grouped by 2 networks of 3 sensors each and 1 network with 2 sensors (GPS network): one network measures temperature and humidity, one measures acceleration and the third one measures GPS coordinates. On the car there is also the gateway of each network linked to a Wrapper that communicate via a WiFi connection with the control room. In particular, we deployed:

1. A TelosB network inside the car, with humidity and temperature sensors (figure7).
2. A MicaZ network with acceleration sensors, outside the car (figure 8). The outside motes are equipped with a box in order to protect them from bad weather conditions.
3. A MicaZ network with a GPS receiver, installed outside too.

The Wrappers and the Mediator run on different laptops and connected via WiFi, the Mediator and the monitoring application are installed in the Control Room.

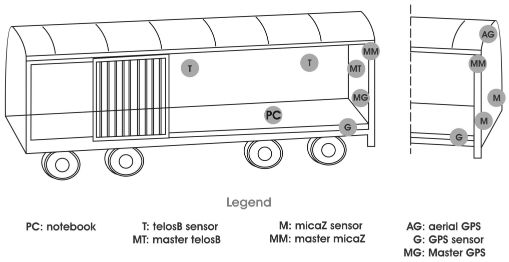

Figure 6: Deployment

We have developed two different applications, respectively for the master and the mote side, they implement a WMECC based security protocol. The master application has been configured in order to digitally sign outgoing query packets addressed to the motes and decrypt the incoming response packets before sending the results to the wrapper. The mote application, in turn, has been configured in order to perform the ECDH protocol initiated by the master, to verify the digital signature of the incoming query packets, and to encrypt all outgoing response packets. The connection among Wrappers and the Mediator implements and SSL protocol.

4.1. Some Experimental Results

In order to test the architecture and demonstrate the functional and security features, different test cases were conduced; we evaluated the parameters sensed by the networks (temperature, humidity, acceleration and GPS coordinates) and we evaluated the packet loss rate on different nodes in two different working conditions:

1. Test 1-Train standing in the station;
2. Test 2-Train running.

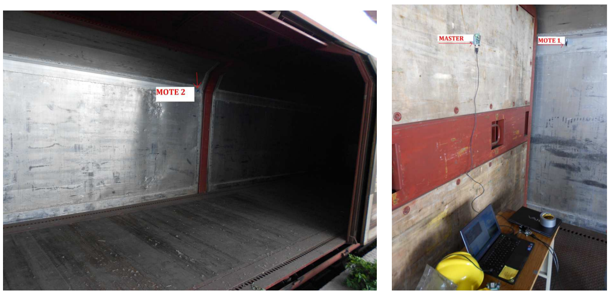

Figure 7: TelosB network

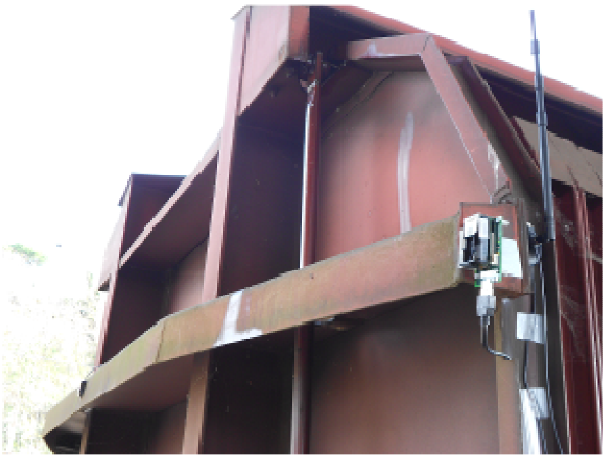

Figure 8: MicaZ network master outside the car

In the following we will illustrate some results of these evaluations, for brevity sake we just illustrate queries concerning only to TelosB network. We want to underline that the goal of this experimental phase was to evaluate the feasibility of the proposed system (WSN hardware and software for the monitoring) and not properly the parameters and values sensed by the different sensors; nevertheless, we will report some of these results, too.

In the Test 1 the train standing in the station. The first test was conduced when the car was standing in the station in order to verify and evaluate the reliability of the connection among nodes; we also evaluated some parameters like temperature and humidity. We assume the TelosB network has two motes with ID 4 and 5. For the first test, we decided to send a query of 5 minutes long (lifetime) with a sample period 0,5 seconds. The network sends back the sensed samples that are collected in a file every 10 seconds (retrieval time) by the wrapper.

Figure 9 shows the evaluated values during the query. The X axis represents the corresponding result file received by the mediator, each result file has samples for 10 seconds of monitoring (retrieval), while the reported values on the Y axis are the mean values evaluated for each file. In table 1 we report the mean values and standard deviation of values for the whole query lifetime and for each sensor. From the result file we can count the number of received samples and easily evaluate the samples loss rate.

Table 1: Sensors mean values

Sensor.Node	Mean	Standard Deviation
Temperature.Node4	19.5 C	0.6
Temperature.Node5	18.06 C	0.8
Humidity.Node4	63.4 %	10.9
Humidity.Node5	61.4 %	4.4

From the result file we can count the number of received samples and easily evaluate the samples loss rate.

According to the query lifetime, the sample period and the retrieval, the mediator should receive 30 result files from network, where the expected number of samples in each of them was 40.

In figure 10 it is possible to see the number of received packets against the expected ones for each node and we evaluated the loss rate of different nodes in the network (figure 11).

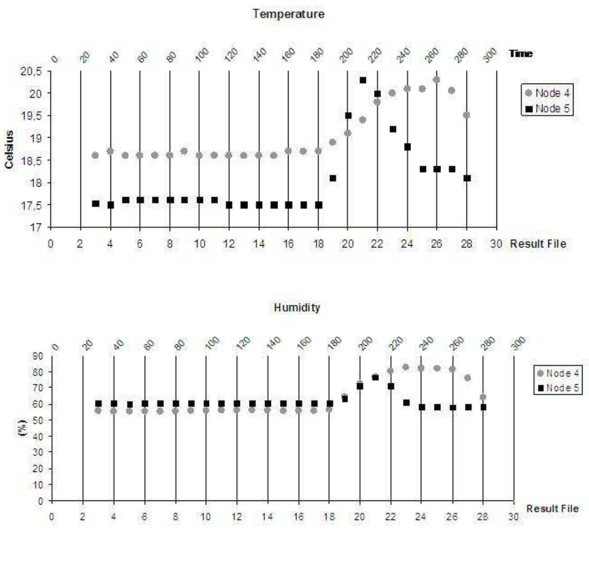

Figure 9: TelosB Network results - Temperature and Humidity

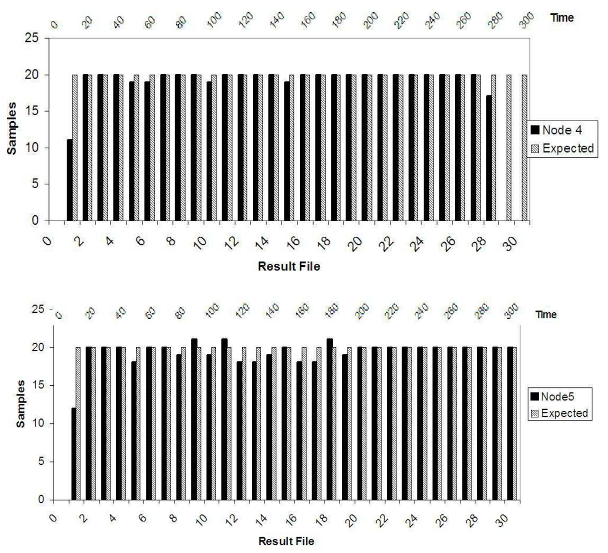

Figure 10: Number of received samples for each node in TelosB

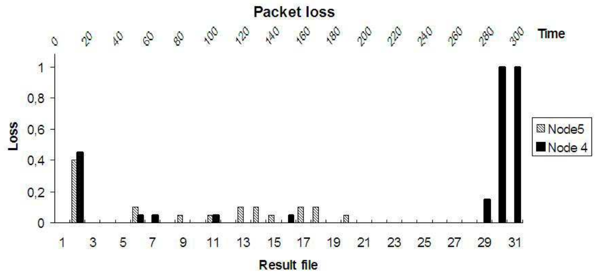

Figure 11: Samples loss rate – TelosB

In table II it is reported the mean number of received samples for each node and for the whole network, evaluated respect of the expected number of samples.

Table 2: Samples Loss

TelosB	Mean
Node4	18
Node4LossRate	9%
Node5	19.4
Node5LossRate	3%
NetLossRate	6%

During the experiment, we decided to stop the node 4, as illustrated in Figure 10 the node loses all samples in the last two files. The node 5 in some intervals has an oversample due to the way SeNSiM aggregates results (e.g. at result file 9, 12 and 18). Both nodes present at the beginning a similar samples loss, this due to the verification of signature in the ECDSA protocol (result file 1).

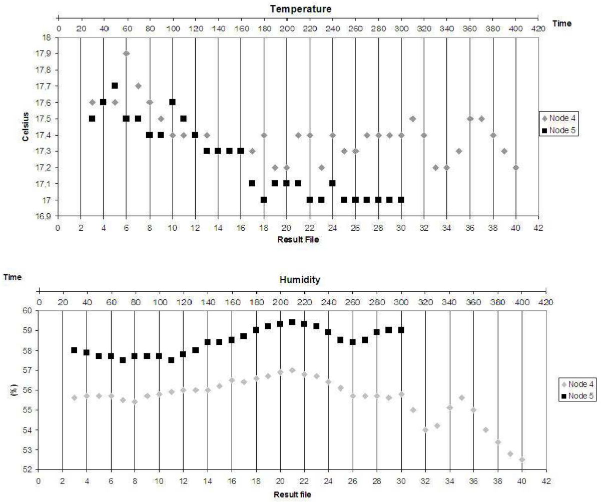

Figure 12: Car in movement – TelosB

In the Test 2 the train is running. The second test was conduced when car was in movement in order to test the connection between nodes and evaluate the measured parameters in a real time condition.

For this test, we sent a query of 7 minutes long (lifetime) with a sample period of 1 second for both networks and 10 seconds of retrieval time. Figure 12 shows the evaluated values during the query for each network.

Again in figure 12 it is reported the case where the Node 5 stacked after the 32th result file and stopped working, this was caused by a not-well closed door that abruptly opened and cut off the node.

In table 3 we reported the mean value and standard deviation of parameters for each network.

Table 3: Sensor mean values for the car in movement

Sensor.Node	Mean	Standard Deviation
Temperature:Node4	17.4 C	0.1
Temperature:Node5	17.2 C	0.1
Humidity:Node4	55.6 %	1.1
Humidity:Node5	58.3 %	0.5

As previously illustrated, we can evaluate the number of received samples and so evaluate the samples loss rate.

According to the query lifetime, the sample period and the retrieval, the mediator should receive 42 result files. For each result file, the expected number of packets for TelosB network was 20.

In figure 13 it is possible to see the number of expected samples for each node and the packet loss rate for the different nodes in the network (figure 14).

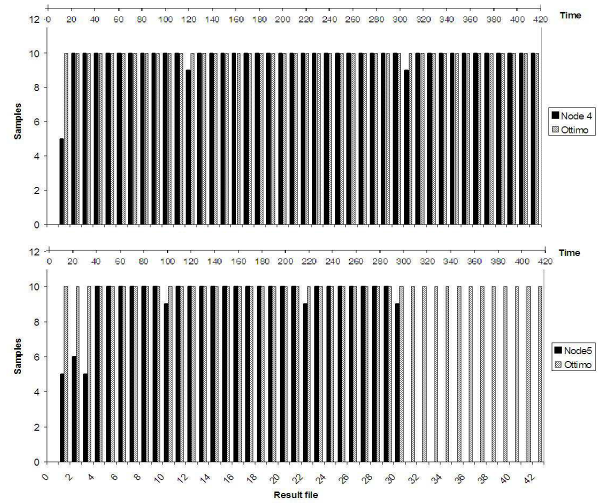

Figure 13: Number of received samples for each node – TelosB

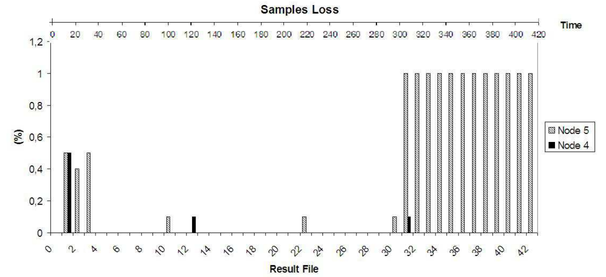

Figure 14: Samples loss rate- TelosB

In table 4 we reported the mean value and standard deviation of parameters for the network under examination.

Table 4: Samples Loss

TelosB	Mean
Node4	9.7
Node4LossRate	2%
Node5	6.6
Node5LossRate	33%
NetLossRate	17%

As the table shows, in this test the network has a good behaviour with a low rate samples loss. Only at the beginning the node lose more samples, always for the ECDSA protocol. We remember that the samples loss of node 5 from 32th result file derives from the accident above mentioned.

5. CONCLUSION AND FUTURE WORK

In this paper we proposed a platform to monitor critical infrastructures as trains. The experimentation performed on the freight car monitoring system provided several useful results. Indeed, we first proved that proposed platform was able to work in a real environment, in presence of harsh operating conditions. Furthermore, the SeNSiM-SEC platform correctly meets the main security requirements by using Cryptography based applications. The security mechanisms do not affect the accuracy of measurements even if a very small delay was introduced in the monitoring activity. Finally, the analisys on network performance was conducted, illustrating that even in running condition, the adoption of wireless sensor networks are feasible on trains. These results motivated our activity and, in next future, we intend to propose more sophisticated monitoring applications based not only on threshold definitions but also on the implementation of decision support systems integrated with available train safety systems.

REFERENCES

A.D. Wood and J.A. Stankovic, 2002. Denial of Service in Sensor Networks, *IEEE Computer,* vol. 35, no. 10, , pp. 54-62.

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

Kapoor V, Sonny V, Abraham Singh R, 2008. Elliptic Curve Cryptography, *ACM Ubiquity*, 9(20): 20-26.

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

Casola V., Esposito M., Flammini F. Mazzocca N., *2012.* Freight train monitoring: a case-study for the pSHIELD project. *Accepted for publication in the proceedings of the Workshop MCNCS 2012, Palermo, Italy.*

R. Rivest, A. Shamir, L. Adleman, 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *In Communications of the ACM*, 21(2).

Hadim, S., Mohamed, 2006. N. Middleware for wireless sensor networks: A survey. *In: Proc. 1st Int. Conf. Comm. System Software and Middleware (Comsware 2006),* New Delhi, India, January 8-12 (2006)

Romer K. 2004. Programming Paradigms and Middleware for Sensor Networks, *GI/ITG Fachgespraech Sensornetze,* Karlsruhe, Feburary 26-27.

Artemis 2011. *The PSHIELD project*, http://www.pshield.eu/

Casola V., Gaglione A., Mazzeo A., 2009. A Reference Architecture for Sensor Networks *Integration and Management in the Book GeoSensor Networks (Proceedings of GSN)* - Springer, LNCS5659

Srivaths Ravi, Anand Raghunathan, Paul Kocher, and Sunil Hattangady, 2004. Security in embedded systems: Design challenges*, ACM Trans. Embed. Comput. Syst.* , 461-491.

Amato F., Casola V., Gaglione A., Mazzeo A., 2010. A semantic eriched data model for sensor network interoperability, *in Simulation Modelling Practice and Theory* 19(8). Pp. 1745-1757, Elsevier.

V. Casola, A. De Benedictis, A. Mazzeo and N. Mazzocca, 2011. SeNsIM-SEC: security in heterogeneous sensor networks, *SARSSI2011*

K. Chebrolu, B. Raman, N. Mishra, P.K. Valiveti, R. Kumar. BriMon, 2008. A Sensor Network System for Railway Bridge Monitoring, *in Proc. 6th International Conference on Mobile Systems, Applications, and Services (ACM MobiSys08),* Breckenridge, CO.

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

Henricksen, K., Robinson, R.A, 2006. Survey of Middleware for Sensor Networks: Stateof- the-Art and Future Directions. *In: MidSens 2006: Proceedings of the international workshop on Middleware for sensor networks,* pp. 6065. ACM Press, Melbourne.

F. Flammini , A. Gaglione, F. Ottello, A. Pappalardo, C. Pragliola, A. Tedesco, 2010. Towards Wireless Sensor Networks for Railway Infrastructure Monitoring, *in Proc. ESARS 2010*, Bologna, Italy, pp 1-6.

H.Wang, B. Sheng, C.C. Tan and Qun Li, 2007. WM ECC: an Elliptic Curve Cryptograph Suite on Sensor Motes, *Technical report*, Oct. 30.