OPEN ACCESS

2nd International Electronic Conference on Sensors and Applications 15–30 November 2015

www.mdpi.com/journal/sensors

Conference Proceedings Paper – Sensors and Applications

Firefighter and Victims Protecting Solution Based on Wireless Body Area Network Nodes

J.A. Sánchez Alcón *, Pedro Castillejo, José-Fernán Martínez and Lourdes López

Research Center on Software Technologies and Multimedia Systems for Sustainability (CITSEM), Universidad Politécnica de Madrid (UPM), Edificio La Arboleda, Campus Sur UPM, C/Alan Turing 3, 28031 Madrid, Spain; E-Mails: pedro.castillejo@upm.es (P.C.); jf.martinez@upm.es; (J.-F.M.); lourdes.lopez@upm.es (L.L.)

* Author to whom correspondence should be addressed; E-Mail: jose.asanchez-alcon@upm.es; Tel.: +34-914-524-900 Ext. 20791.

Published: 10 November 2015

Abstract: Interconnectivity between web systems and sensor networks is useful to provide smart services for the Internet of Things. These services are based on data collection and processing to obtain useful information about the supervised environment. Using this information it is possible to provide smart services, but some of them must be considered as protected by the legislation regarding privacy of personal data. In order to face this issue, security and privacy mechanisms must be used. So as to deal with the limited resources in sensor networks, these mechanisms must be as lightweight as possible to preserve the enough Quality of Service. However, these mechanisms must fulfill security and privacy requirements defined by the regulations. This paper describes a Wireless Body Area Network application providing services to protect firefighters work in hazardous environments. The firefighter wears a special shirt with sensors embedded. These sensors are able to monitor not only the firefighter health status, but also they can be connected to external sensors in order to monitor the health status of the victims. These external sensors are part of the equipment carried by the firefighter to face the emergencies and save lives. Finally, using this solution they are able to obtain external medical aid.

Keywords: Internet of things; security; privacy; trust; wireless body area network; health monitoring

---

1. Introduction

In this paper we propose a service to protect firefighters and victims by means of a Wireless Body Area Network (WBAN) used by the fire brigades in hazardous environments. It is based on a special shirt with sensors embedded that are able to monitor the firefighter health status. In addition, these wearable sensors can be connected to external sensors in order to monitor the health status of the victims. The external sensors are part of the equipment carried by the firefighter in order to obtain external medical aid so as to provide a safe rescue procedure to victims. The basic structure of the service is depicted in Figure 1 where the key elements are included. There are two different actuations roles. The first one is the "rescue team", where each firefighter carries a wearable sensor to gather the vital health parameters [1] and act as a cluster head for the sensors placed on the victims found. The cluster heads are able to assist each other, and all cluster heads can find the best route to the gateway, either directly or via cluster heads neighborhood. Thus, the health status of all the persons involved in the rescue (firefighters and victims) is controlled by medical staff, giving the appropriate directions oriented to save their lives. The second role is the "support team", which receives and identifies the victims, and carries them to a safe place.

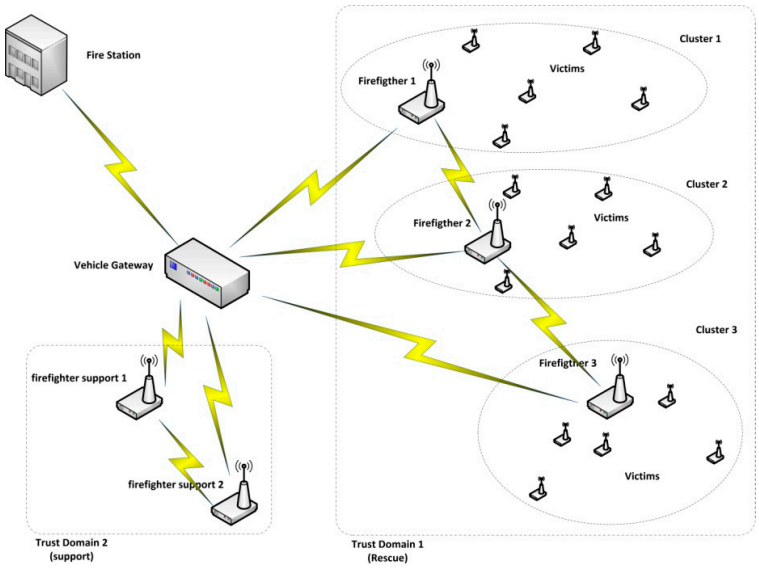

Figure 1. Firefighters team, in emergency actuation carrying wireless body sensors.

2. Analysis of the Requirements Regarding Security Privacy and Trust on Data Gathered

As presented in the 2014 conference paper titled "Automatic System for Providing Security Services in the Internet of Things applications over Wireless Sensor Networks" [2], the security and privacy protections are regulated by laws [3]. In the case of Spanish and European regulations the trend is to construct a DPIA-T (Data Protection Impact Assessment – Template) [4] for each service. Previously, it is necessary to know some high level information about the service called Utility Matrix in [2], which is divided in two groups as we can see in Table 1 where both the service and the network type that supports the services are defined. The security and privacy imperatives in DPIA-T format [4] are as follows: 1- Data related health status is considered as personal data that must be protected. 2- Data must be as fresh as possible and true. 3- Critical data for safety the life are priority.

Table 1. Utility Matrix: Service and Network type for the service.

UTILITY MATRIX: Description		**Network Type**	
Service name	Firefighter and victims protecting	Network name	NW_Type1
Service Type	Health-care; Safety	Mote resources limit	Wearable mote: Memory to store data on standalone operation
Environment Type	Emergency	Connectivity	Radio
Country	Spain	Communications	
Promoter	Government	BS resources limit	None
User	Firefighter	Topology	Mesh for Cluster heads, Star between victims motes and the cluster head
Monitored person	Firefighter and victims.	Nodes Roles	Gather health and environment parameters
Legal capacity of person	Variety of cases	Routing	Hieratical based on cluster heads
Special needs person	Variety of cases		
Continuity of service	Yes; (standalone operation)		
Critically of the service	high		

The legal imperatives over sensitive information are structured as shown in Table 2, and the specific protections to data set are assigned in the Table 3.

Table 2. Legal imperatives in DPIA-T format.

DPIA-T : Firefighter and victims protecting solution.			
Security service	**Attack**	**Target**	**Defence**
Availability	DoS	1- The physical layer is degraded and the communication among nodes is impossible (jamming). 2- A spurious node starts sending malicious data packets to the network.	It must be known the situation for to face it.
Authentication	Sybil	A node is asking for multiple IDs, and if the attack succeeds, the node is able to subvert the trust mechanism.	Restore trust mechanism rejecting the malicious node.
	Node replication	When a node ID is copied, replicated in a new node, and then introduced in the network. From that moment on, the network accepts the node with the cloned ID as an authorized node.	Realize and revoke the malicious node.
	False node	It introduces data traffic in the network to avoid legitimate nodes to communicate (injecting false data messages, claiming for authorization continuously, *etc.*).	Identify the false node and discard all messages.
Integrity	Message corruption	When a message reaches the recipient with a different content than the one sent by the source. This situation is either because the message has been degraded in the transmission, or because the message has been intercepted and intentionally changed.	Ensure that messages have not been altered.
Privacy	Eavesdropping	Other devices listening in the same frequency may intercept every communication between two nodes.	Provide authentication and ciphering capabilities. Use data anonymization.
	Node subversion	When a node is captured and cryptoanalyzed the secret keys, node ID, security policies, and so forth are disclosed.	Use few data stored in each node and renew the keys.

Table 3. Data protection over data sets and trust domains defined.

Sensor		**Measures**	**Type**	**Auth**	**Integr**	**Privacy**	**Avail**	**Intruders insiders**	**Trust domain**
1	Firefighters	CO; Smoke; Gas	Vital for life	X	X	-	X	X	Domain 1
2		Temperature heart rate	Private information	X	X	-	X	X	
3	Victims	Temperature heart rate Oxygen saturation		X	X	-	X	X	
4	Firefighters Victim Support	Temperature heart rate Oxygen saturation personal identification		X	X	X	-	X	Domain 2

Regarding security services and mechanisms designed for this type of service and network, the expert system module TSES knowledge base [2] was already defined (among many others) and the SensoTrust proposal security structure [5] has been chosen, which is based on trust domains definition where each of them has a common security policy [6,7]. Two trust domains have been defined: one for the rescue team (Domain 1) and the other for the firefighter support team (Domain 2), selecting the Domain Key Servers (as presented in SensoTrust proposal [5] in both domains using the cluster head

nodes. Once the protections to data regarding the service have been assigned, the expert system [2] must find the appropriate mechanisms in its knowledge base to face the attacks mentioned in DPIA-T. As already presented in Table 3, there are two major types of security and privacy requirements. After applying the legal imperatives (DPIA-T) to the current case, the following list of security and privacy mechanisms appears, taking into account that it can be applied as the common scheme indicated (key distributed, roles and trust policies) in SensoTrust [5]. Trust domain policies are shown in Table 4. Countermeasures against outsider attacks are based on authentication, and the countermeasures against insider attacks are based on the security policies and the trust domains.

Table 4. Trust domain policies**.**

		Domain 1 policy	**Domain 2 policy**
Security service	**Attack**	**Countermeasure**	**-**
Avail.	DoS	One alarm is triggered in the Security Manager informing about the situation	-
Authent.	Sybil	In The security scheme, every node ID is preconfigured for each node and only the Security Manager (out of the WSN) has the complete list of the IDs. In extremis, it is possible to perform a node revocation.	
	Node replication	The Node ID is stored in an external entity (SM) that controls all the IDs working in the network. Security policy, if the SM detects that 2 nodes are operating with the same ID, a node revocation protocol is issued, and the node is dropped from the network.	
	False node	Using the node ID, the schema is able to identify the false node and, using the domain key renewal functionality, all the messages sent by this node will be discarded.	
Integ.	Message corruption	To avoid both issues, security schema includes the ciphering suite functionality, which allows performing a message hash (using MD5, SHA1, *etc.*).	
Priv.	Eavesdropping	-	To avoid data disclosure, It provides both symmetric and PKI ciphering capabilities. Anonymization, unlink the personal identification and his/her measure data
	Node subversion	-	To avoid it is to minimize the cryptographic and security information stored in each node. Nevertheless, all the keys in the network can be renewed.

3. Results and Discussion

To preserve the Quality of Service (QoS) it is necessary to know the restrictions. Sensors 1-3 (firefighter and victims) have as critical requirements both battery consumption and delay, but this does not applies to sensor 4 (Firefighters victim Support). The results obtained in laboratory tests are presented in Figure 2. Finally, it is necessary that the system provides reports about both the anomalies found (attack detections as a result of true positives, true negatives, false positives and false negatives) and their reactions. The reporting to BES and TSES is composed by: 1- no legislation-based impact attacks; 2- seriousness of the impacts; 3- legislation-based impact and 4- alarm report.

Reporting to LES is composed by legislation-based impact and improvement plan report. Some indicators [8] are defined as the Percentile 90 over the time until fault resolution, considering MTBF (Mean Time Between Failures) as true positives and false negatives, and MTTR (Mean Time To Repair) as true positives, false negatives and false positives (as the resources spent on inefficient results). The actuations on false negatives represent the impact when a problem is not detected on time. Then, Coef(no attacks) => MTBF / (MTBF + MTTR).

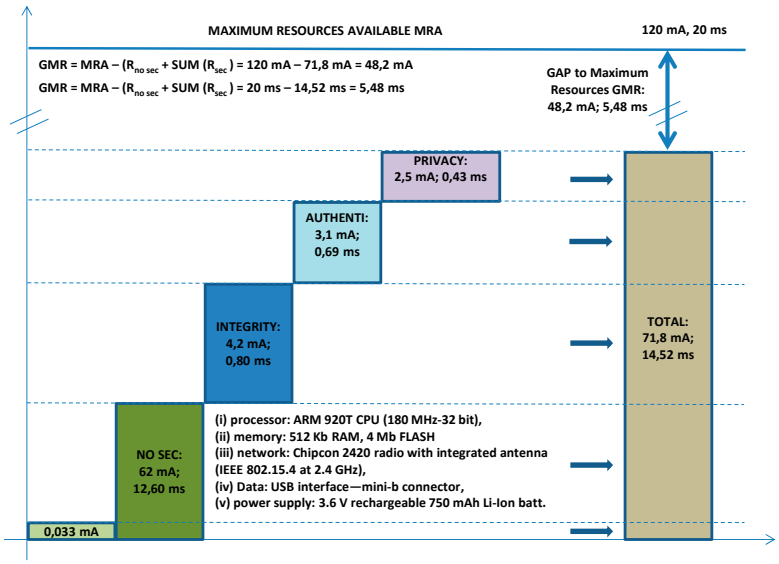

Figure 2. Energy spent *vs.* security services, and d delay *vs.* security services.

4. Conclusions

In this paper we have proposed a service able to protect firefighters and victims using a Wireless Body Area Network ported by the fire brigades in hazardous environments.

In order to protect the Quality of Service of the system and fulfill the security and privacy requirements requested by laws it is necessary to provide a tailored security and privacy solution [2]. The security structure and the mechanisms to apply must be as lightweight as possible [6,7]. In the presented use case of this solution, the expert system proposed in our last conference paper selected SensoTrust proposal [5] as one of the best solutions to build the security and privacy solution. It is also necessary to monitor service performance both in the resource consumption and the protection offered.

So as to provide a continuous service enhancement, it is necessary to implement an adequate strategy of supervision over the key performance indicators. This supervision must be established over the *quality of the equipment involved* (hardware, software and communication among them), the *quality of service* (functionality) and the *quality of security and protection* (security services and mechanisms). All of them must be analyzed together in order to obtain the desired results.

Acknowledgments

The authors would like to thank CITSEM (Research Center on Software Technologies and Multimedia Systems for Sustainability, Centro de Investigación en Tecnologías Software y Sistemas Multimedia para la Sostenibilidad) from the UPM. The work presented in this paper has been supported by *AWARE* project (partially funded by the Spanish Ministry of Economy and Competitiveness with reference TEC2011-28397) and *LifeWear* project (funded by the Spanish Ministry of Industry, Energy and Tourism with reference TSI-010400-2010-100.

Author Contributions

All the authors contributed equally to this work.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Rolim, C.O.; Koch, F.L.; Westphall, C.B.; Werner, J.; Fracalossi, A.; Salvador, G.S. A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. In eHealth, Telemedicine, and Social Medicine 2010, Proceedings of the ETELEMED '10. Second International Conference, Location of Conference, 10-16 Feb. 2010, pp.95-99. DOI: 10.1109/eTELEMED.2010.19.
2. Alcón, J.; López, L.; Martínez, J.; Castillejo, P. Automatic System for Providing Security Services in the Internet of Things applications over Wireless Sensor Networks. In Proceedings of the 1st Int. Electron. Conf. Sens. Appl., 1–16 June 2014; Sciforum Electronic Conference Series, Vol. 1, 2014, d005; doi:10.3390/ecsa-1-d005
3. European Commission. Opinion 8/2014 on the on recent developments on the internet of things, n. 14/EN WP 223, adopted on 16 September 2014, pp. 1-24. Available online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (accessed on 23 September 2015)
4. Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, 18.03.2014. . Available online: https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf, (accessed on 24 September 2015).
5. Pedro Castillejo, P.; Martínez-Ortega, , J.F; López, L; Sánchez Alcón, J.A. SensoTrust: Trustworthy Domains in Wireless Sensor Networks IJDSN 2015, Article ID 484820, 10 pages. doi:10.1155/2015/484820
6. Farooq, A.; Petros, M. Security for wireless ad hoc networks, Publisher: Wiley-Interscience, cop. 2007; 247p.
7. Cazorla L.; Alcaraz, C.; Lopez, J. Towards automatic critical infrastructure protection through machine learning. In Proceedings of 8th International Conference on Critical Information Infrastructures Security, Amsterdam, The Netherlands, September 16-18, 2013; Springer: 2013; LNCS 8328, pp. 197-203, doi: 10.1007/978-3-319-03964-0_18. Available online: http://link.springer.com/chapter/10.1007%2F978-3-319-03964-0_18#page-1 (accessed 12 September 2015)
8. Herrmann; Debra S. Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI; Publisher: Boca Raton Florida, 2007; 824p. ISBN 978-0-8493-5402-1