Firefighter and victims protecting solution based on Wireless Body Area Network nodes

Autores:

J.A. Sánchez Alcón: jose.asanchez-alcon@upm.es
Pedro Castillejo: pedro.castillejo@upm.es
José-Fernán Martínez: jf.martinez@upm.es
Lourdes López: lourdes.lopez@upm.es

INDEX

1. Antecedent and Objectives
2. The service
3. Utility Matrix
4. Security and privacy Imperatives
5. Requirements: Security / Privacy and QoS
6. Conclusions and results
7. Future works

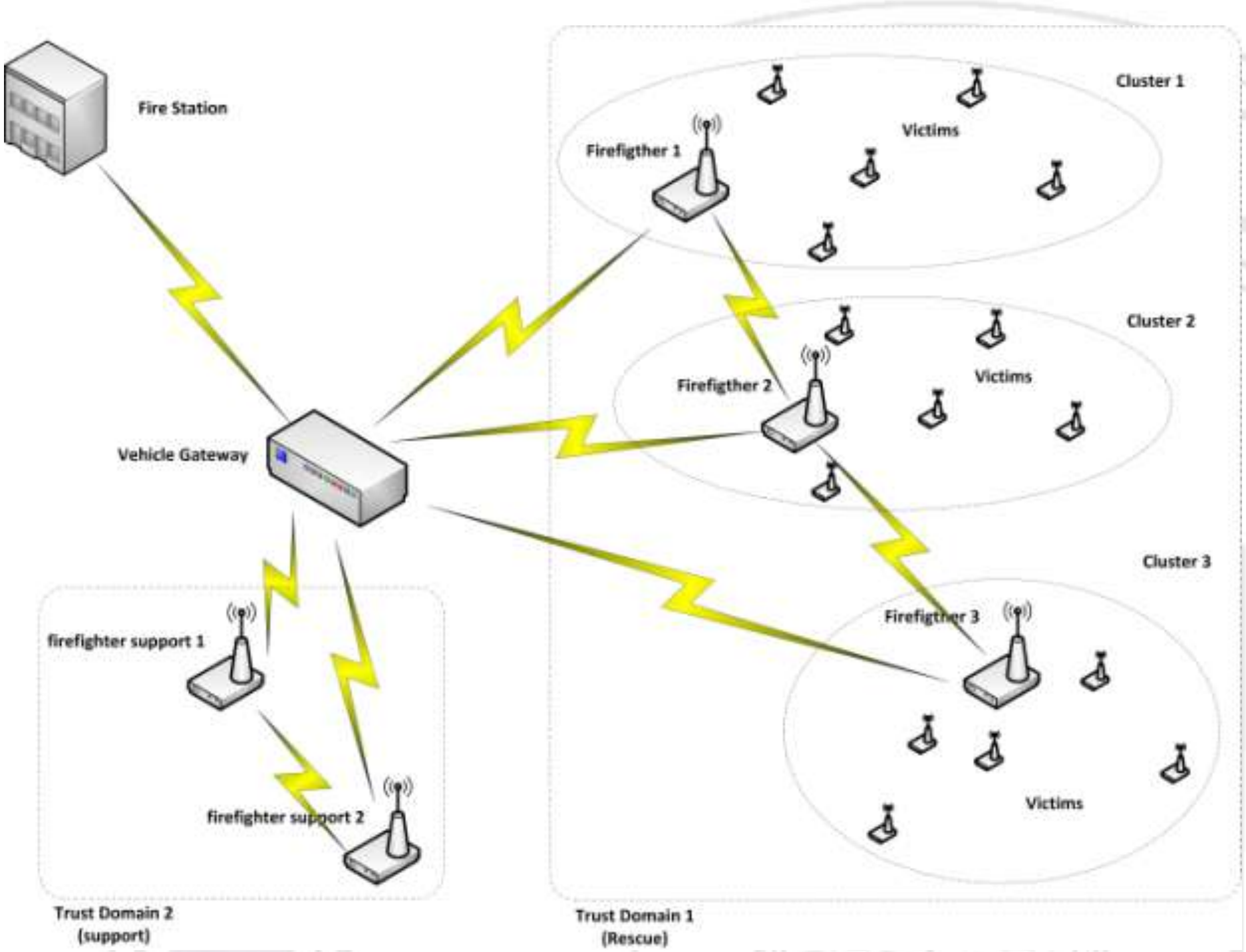
Antecedent and Objectives

- Some of the contributions in this paper are based on the results presented in (http://sciforum.net/conference/ecsa-1/paper/2408)
- Two of the main topics to be considered are:
  - The Quality of Service (based on service requirement) and,
  - The protection of the personal data involved (based on law requirement).
- As result one possible solution to satisfy both topics must be provided.
- To ensure the required performance, both topics must be supervised in order to obtain the enough reliability.

The service

Supervise the health for firefighters and victims:

- WBAN application to protect firefighters work in hazardous environments.
- The firefighter wears a special shirt with sensors embedded and also they carry external sensors to monitor the victims' health status in order to obtain the proper medical aid.



Utility Matrix

Utility matrix is a set of information about the proper service and the main technical characteristics of the network type.

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		

This information is enough to select both the legal framework and the network structure.

Security and privacy Imperatives

With the Utility matrix description and network type, Data Protection Impact Assessment Template is defined as the set of imperatives on security and privacy.

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.

Requirements: Security / Privacy and QoS

To preserve the Quality of Service (QoS): Sensors 1-3 (firefighter and victims) have as critical requirement both battery consumption and delay, but not for sensors 4 (Firefighters Victim Support).

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

Conclusions and results

The countermeasures against outsider attacks are based on authentication, and the countermeasures against insider attacks are based on the security policies and trust domains.

		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.

Future works

- In order to protect the Quality of Service and satisfy the security and privacy requirements by laws at the same time is necessary to provide a tailored security and privacy.
- The security structure and the mechanisms to apply must be as lightweight as possible.
- In this use case of this service, expert system proposed in the last conference has selected SensoTrust proposal as one of the best solutions to build the security and privacy solutions.
- It is also necessary to monitor service performance both in the resource consumption and the protection offered, launching reports to engineering and maintenance staffs.

Thanks for your attention