Using Behaviour Trees to Verify Protocols in Complex Sensor Networks

Kalvinder Singh [#1], Vallipuram Muthukkumarasamy [*2]

[#] *IBM, Australia Development Lab, and Griffith University*
Gold Coast, Australia
[1] kalsingh@au.ibm.com

[*] *School of Information and Communication Technology, Griffith University*
Gold Coast, Australia
[2] v.muthu@griffith.edu.au

I. Abstract

Information assurance, privacy and other requirements of sensor systems is complex. Proposed sensor systems contain many different components and hence are inherently complex. The complexity hinders security proofs and analysis, so that proving a protocol is secure within an entire system is rarely performed. Instead researchers only show a sub–system is secure, for instance, communication between two or three nodes. We show how Genetic Design Methodology can effectively model the security requirements of a sensor system, and be used to model and show the security of a complex sensor system.

A home health care system, with both body and external sensors is an example of a complex sensor network system. The complexity of the system increases as we add more sensors to obtain more data. For instance, blood pressure increasing due to exercise is normal. However, increase in blood pressure while at rest could mean a serious medical condition. Sensors may not just measure physiological values, but also body motions, which can lead to a number of different sensors needing to communicate with each other. As the number of heterogeneous sensors increases, so will the complexity of interactions between the sensors.

Figure 1 gives a diagrammatic representation of a home automation system that can be used in monitor the elderly. The diagram shows the communication of the sensors with the central home controller. The home controller is a specialized device that is situated at home and is connected to the internet. In the case where this system is part of a health system, the home controller is a specialized device that communicates the necessary information to the hospital. Depending on the health risks and privacy concerns of the patient all of the information may not be transmitted to a hospital. For instance, cameras (home sensors) may only start recording if the body sensors detect that there may be a medical emergency, such as the patient lying horizontal in the kitchen. Surveillance software can be used to detect if the patient is cleaning the kitchen, or getting something from the ground, or there is actually an emergency. If the software does detect an emergency, the hospital staff is notified; they examine the information, and decide on the best course of action.

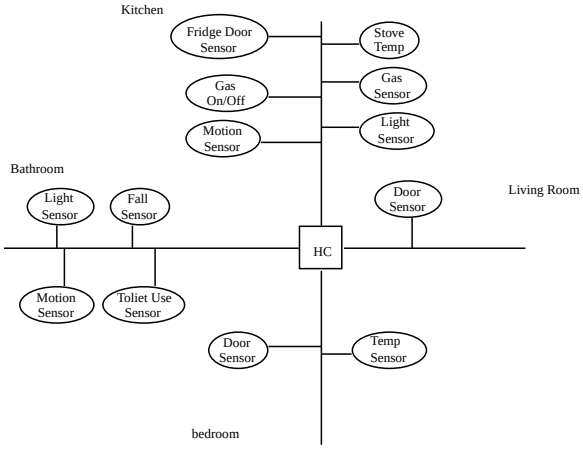

Fig. 1. Home Automation System

References

[1] K. Singh and V. Muthukkumarasamy, "A minimal protocol for authenticated key distribution in wireless sensor networks," in *ICISIP '06: Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing.* Bangalore, India: IEEE Press, December 2006, pp. 78–83.

[2] K. Singh, K. Bhatt, and V. Muthukkumarasamy, "Protecting small keys in authentication protocols for wireless sensor networks," in *Proceedings of the Australian Telecommunication Networks and Applications Conference*, Melbourne, Australia, December 2006, pp. 31–35.

[3] K. Singh and V. Muthukkumarasamy, "Performance analysis of proposed key establishment protocols in multi–tiered sensor networks," *Journal of Networks*, vol. 3, no. 6, 2008.

[4] K. Singh and V. Muthukkumarasamy, "Key establishment protocols using environmental and physiological data in wireless sensor networks," *Inderscience International Journal of Sensor Networks IJSNet*, accepted with Minor Corrections.

[5] K. Singh and V. Muthukkumarasamy, "Verification of key establishment protocols for a home health care system," in *Proceedings of the Fourth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Sydney, Australia, December 2008.

[6] K. Singh and V. Muthukkumarasamy, "Implementation and analysis of sensor security protocols in a home health care system," in *Proceedings of the Third International Conference on Network and System Security*, Gold Coast, Australia, October 2009.