# An Immunology Inspired Approach to Robust Sensor Networking

Tatiana Bokareva[1,2]
The University of NSW[1]
Email: tbokareva@cse.unsw.edu.au
National ICT Australia Limited[2]
Bay 15, Australian Technology Park
Eveleigh, NSW 1430, Australia

Nirupama Bulusu[3]
Portland State University[3]
Portland, OR 97207, USA
Email:nbulusu@cs.pdx.edu

Sanjay Jha[1,2]
The University of NSW[1]
Email: sjha@cse.unsw.edu.au
National ICT Australia Limited[2]
Bay 15, Australian Technology Park
Eveleigh, NSW 1430, Australia

*Abstract*— **For widespread adoption of sensor technology, we must ensure that sensor networks are robust in the event of abnormal behavior such as a network intrusion or failure of components or nodes. Current research on robust and resilient sensor networking is focused on low-level security primitives such as secure broadcast or localization for small groups of sensor nodes. What has been lacking is a comprehensive, whole-network approach to sensor network robustness across diverse, unknown failure modalities.**

**We are exploring an immunologically inspired approach to robust sensor networking. The key idea is to build a sensor network that can distinguish between normal and deviant behavior by maintaining a notion of ”self”, like the natural immune system.**

**SASHA is our self-healing hybrid sensor network architecture that is intended to provide automatic fault recognition and response over a wide range of possible faults. We envision SASHA to have an ability to learn and evolve its monitoring and inference capabilities with time.**

## I. Introduction

Wireless sensor networks are a growing focus of the research community, due to their potential to embed sensing and communication in a wide variety of environments. One of the most valuable applications of wireless sensor networks is in the deployment of nodes in hostile or remote geographical locations, given the systems ability to operate unattended, without pre-existing infrastructure and with minimal or no maintenance [2]. Due to their operational environment, sensor nodes are subject to frequent failures. For widespread adoption of sensor technology, it is critical that a system can heal itself in the event of abnormal behavior such as a network intrusion, or failures of components or nodes.

Previous work on robust and resilient sensor networking is focused on specific tasks, such as secure broadcast[7], secure aggregation[8], secure localization[6], or fault-tolerant feature extraction [5]. Such primitives constitute indispensable building blocks for sensor networks. But how should we use and combine these primitives? For example, sensor data can be corrupted by malicious sensors, as well as faults induced by physical world coupling. Sensor calibration techniques can compensate for faulty sensor readings, but cannot account for malicious aggregator nodes. Secure aggregation can protect against malicious aggregators, but cannot detect persistent faults in sensor data[3]. Consequently, in each case, only one type of failure modality is addressed. In this case, what is required is a comprehensive approach to fault-tolerant data collection across various failure modalities. In general this motivates a whole-network approach to sensor network robustness that operates above the network layer (Figure 1).

How do we build such a comprehensive fault tolerant system in an efficient manner? One possible solution may lie in the natural immune system which is remarkably autonomous, compact, robust and adaptive to unknown and diverse pathogens. Forrest [1] first advocated immunology inspired solutions for robust computer systems. We are building SASHA a self-healing hybrid sensor network architecture that is inspired by and co-opts several mechanisms from the natural immune system.

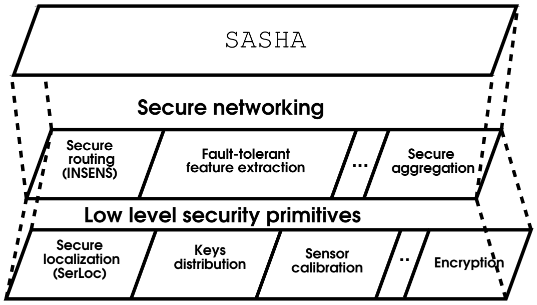

Fig. 1. SASHA: A knowledge plane for a robust sensor network.

## II. SASHA Architecture

### A. Self in Sensor Networks

One of the main roles of the natural immune system is the recognition of self and the elimination of non-self proteins. In modeling an immune system equivalent for a sensor network, we must have a clear and stable definition of what constitutes the self and non-self sets. This is challenging for wireless sensor networks, because each application has its own unique characteristics and requirements. Nevertheless, we can identify several similarities that belong to an entire family of wireless sensor network applications such as: (i) sensor nodes are usually deployed with a common goal in mind, (ii) sensors generate data streams and (iii) sensor nodes may be subject to frequent failures. Based on the assumptions outlined above we define the notion of self for a sensor network to consist of

1) Correct sensor readings.
2) Appropriate behavior of a running application event.
3) Authenticated set of neighbors.

### B. System Architecture

Our self-healing sensor network architecture is envisioned to comprises of several coordinating components, namely: a large number of sensing nodes, several monitoring nodes, base stations, a Thymus machine, and a Lymph (database) machine.

**Sensing nodes:** Sensing nodes are small, resource-constrained sensor nodes such as the Mica mote. They organize themselves into a network, sense and relay real-life measurements toward the closest monitoring nodes. In other words, nodes will organize themselves into trees, with each tree rooted at a monitoring node. We plan to build on previous research in sensor network self-organization to construct efficient protocols for construction and maintenance of such trees[4].

**Monitoring Nodes:** Monitoring nodes have enhanced sensing, processing and communication capabilities such as the Stargate. It is desirable that they have two communication channels, one to communicate with sensing nodes, and the other to communicate among themselves. Each monitoring node covers a portion of the network topology. As a simple example, in order to build and maintain a notion of *self* for the task of fault tolerant collection of temperature measurements, one of the monitoring node's responsibilities is to identify faulty sensor readings. This task will be accomplished by means of using *Self-Organizing Neural Network with Competitive Learning (SONN)*. For the monitoring nodes to detect anomalies, we need to identify rules based on which distinction between normal and malicious behavior can be made. The competitive learning network archives this by dividing a set of input parameters into data clusters and by choosing the winning one. SONN learns to categorize an input vector it sees based on the simple *Kohonen learning rule*

$$w_i(t+1) = w_i(t) + \lambda \times (m_i(t) - w_i(t)) \tag{1}$$

where $w$ is a weight vector, $m$ is an input vector and $\lambda$ is a learning rate. As a result, SONN will output a vector $O = [o_1, ..., o_n]$ with $0s$ for all neural inputs except the most positive element, which corresponds to a *winning* neuron. The output for the winning neuron is set to 1.

$$o_i = \begin{cases} 1 & \parallel w_i(t) - m_i(t) \parallel \leq \parallel w_o(t) - m_i(t) \parallel \forall o \\ 0 & \text{otherwise} \end{cases}$$

**Lymph:** One of the major components of the natural immune system are B cells, a form of white blood cell. These cells are programmed to look for certain kinds of disease-causing pathogens, then destroy them and the cells infected by them. In a sensor network, to detect anomalies, the survey of a forest of trees can be undertaken by means of mobile scripts running on all monitors, called a B-script. A script is dynamically generated code and it will perform statistical analysis of a tree. For example, for fault tolerant temperature data collection, once the training period of SONN is over the Lymph machine will generate a monitoring script and send this script to the monitoring node. This script will survey outputs of the SONN in order to detect abnormal sensor readings.

**Thymus:** In the thymus gland of the immune system, what are known as the T-cells undergo a process of maturation prior to release into the circulation. This process allows the T-cells to develop an important attribute known as self-tolerance. Likewise, the Thymus machine in SASHA is reserved for the representation of *self.* If an abnormality is detected its corresponding representation will be sent to the Thymus machine. The anomaly will be compared to other instances of self stored on this machine. If a match is not found then the Thymus machine will respond with a *co-stimulation* packet back to the monitoring node. The role of the co-stimulation packet is to confirm an anomaly and possibly trigger a network response to the anomaly.

**Base Station:** The role of the base-station is to provide a solution to the attack to monitoring nodes, collect sensor data and request updates on the Lymph and Thymus machines.

All these different entities are indispensable to SASHA. The system complexity and resource requirements increase progressively from sensing nodes, monitoring nodes, to base station, Lymph and Thymus.

### C. *SASHA Functions*

SASHA has three specific aims:

1) *Automatic fault recognition* consists of a lightweight, distributed learning algorithm to recognize faulty sensor readings and other types of anomalies from deviant characteristics in its self-set (correlations with current sensor state of neighboring nodes, abnormal variations in sensor data stream characteristics).
2) *Adaptive network monitoring* consists of an algorithm for generation, maturation and migration of mobile monitoring scripts. We can use genetic algorithms to generate a continuously changeable set of scripts based on the existing representation of a non-self set stored on the Lymph database.
3) *Coordinated Response* consists of the response to malicious or faulty behaivour accomplished via coordination between monitoring nodes, or between monitoring nodes, Lymph, Thymus and Base station.

## III. Conclusion

In this paper, we described our immunology-inspired approach to robust and resilient sensor networking. Instead of focusing on protocols to support specific security primitives such as secure localization or secure aggregation, we are building a holistic system architecture called SASHA, that is inspired by and co-opts several mechanism from the natural immune system, to attain its autonomy, robustness, diversity and adaptability to unknown pathogens.

Several challenges must be met to achieve a complete realization of SASHA, including the design of (i) learning algorithms to support automatic fault recognition and response, and (ii) genetic algorithms to support evolution of its monitoring and inference capabilities over time. Nevertheless, we believe this architecture constitutes an important step toward robust and resilient sensor networking.

## References

[1] Steven Hofmeyr Anil Somayaji and Stephanie Forrest. Principles of a computer immune system. In *Proceedings of New Security Paradigms Workshop*, Cumbria, UK, November 1997.

[2] Edited by D. Estrin and W. Michenerand G. Bonito. Environmental cyberinfrastructure needs for distributed sensor network. *Scripps Institute of Oceanography*, Agust "12–14" 2003.

[3] Saurabh Ganeriwal and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*, pages 66–77. ACM Press, 2004.

[4] Wen Hu, Nirupama Bulusu, and Sanjay Jha. A communication paradigm for hybrid sensor/actuator networks. In *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC 2004)*, Barcelona, Spain, 5-8 September 2004.

[5] Bhaskar Krishnamachari and Sitharama Iyengar. Efficient and fault-tolerant feature extraction in sensor networks. In *Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03)*, Palo Alto, California, April 2003.

[6] Loukas Lazos and Radha Poovendran. Serloc: secure range-independent localization for wireless sensor networks. In *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*, pages 21–30. ACM Press, 2004.

[7] Adrian Perrig, Robert Szewczyck, Victor Wen, David Culler, and Doug Tygar. Spins: Security protocols for sensor networks. In *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (ACM MOBICOM '01)*, pages 189–199, Rome, Italy, July 2001. ACM.

[8] B. Przydatek, D. Song, and A. Perrig. Sia: Secure information aggregation in sensor networks. In *Proceedings of the ACM SenSys 2003*, Los Angeles, CA, November 2003.