Impact of Misbehaviour and its Detection in Ad-hoc Wireless Sensor Networks using AIS

Sven Schaust, Martin Drozda, Helena Szczerbicka
FG Simulation und Modellierung
Institute of Systems Engineering
Leibniz University of Hannover
{svs,drozda,hsz}@sim.uni-hannover.de

1 Motivation

Characteristic for ad-hoc wireless sensor networks is the lack of a centralized control. Instead each node serves as a routing device, which is able to forward packets to its neighbors[1] and receive packets from them. Node movement is allowed, but rare for sensor nodes. Each node is able to be switched on and off at any time depending on its power saving configuration. Such networks are extremely vulnerable to user misbehavior. Since nodes within an ad-hoc sensor network are expected to have limited computational power and be battery powered, a system that is going to protect them has to be *lightweight*. It has to be adaptive too, as ad-hoc sensor networks are expected to operate autonomously with only spare maintenance. Classical intrusion detection approaches which are based on intrusion signatures therefore do not apply for such a task.
Artificial immune systems (AIS) on the other hand seem capable of handling such demands. AIS are inspired by the *Human immune system* (HIS) using selected features of this defense system. The basic feature of an HIS is the ability to discriminate between *self* and *non-self*. In case of sensor networks non-self is any kind of user behavior that impacts the network in a negative way. The purpose of our simulation based experiments is to show that AIS are a suitable approach for detecting misbehavior in ad hoc sensor networks.

2 Artificial Immune System

Artifical immune systems (see [2], [9]) are inspired by the Human immune system. The latter one is a complex mechanism which is able to protect humans against a variety of virological and bacteriological attacks. The system's capabilities to differentiate between *self* and *non-self* is remarkable. Due to evolutionary development the human body has gained an innate immune system and a system which is able to adapt and learn to detect and neutralize new kinds of attacks.

2.1 Adaptive Immune System

The adaptive immune system is the source of inspiration when it comes to artifical immune systems. The cells involved in this system are called T- and B-cells. The first ones are produced in the thymus, while the latter ones are produced in the bone marrow. These cells are able to bind to specific structures (or surfaces) of attackers (*antigens*), thus building up an effective defense line. Whenever a T-cell binds to an antigen a response is triggered which involves B-cells to eliminate the antigen. Due to a sophisticated learning process the immune system is able to memorize attackers and to respond faster the next time.

2.1.1 Learning Phase

T-cells are covered by receptors that are able to bind antigens. These cells are produced by a random process in the thymus. After surviving a negative selection process[2] the T-cells are injected into the body. A reaction is forced when T-cells bind with a possible non-self antigen. If the non-self is classified as harmful an immune reaction is triggered by T- and B-cells. The T-cells start to divide and mature over time, also producing memory T-cells. These are highly specialized long living cells and if activated by antigens cause a steady and fast immune reaction. Mature B-cells are able to produce antibodies. These match only specific antigens of known attackers. Vaccination is an artifical process to stimulate such a response and production.
See [4] for more details on the human immune system.

[1] Nodes within radio range of the sender.

[2] Cells must not recognize self.

2.2 AIS Algorithm

An Artificial immune system normally reflects typical behavior of the Human immune system by collapsing different sorts of T- and B-cells into a single entity called detector.
AIS Algorithm:

1. Create self-set
2. Create detector with pseudo-random process
3. Check detector against self-set. If it does match, throw detector away. If not add detector to detector-set.
4. Compare suspected non-self strings with detectors. If it matches trigger response. If the response is triggered quite often, mark detector as memory (T-cell) detector.
5. Clone and randomly change the detectors binding capabilities to produce new detectors.

3 Misbehavior detection with AIS

In accordance with the literature, see e.g. [3], we represent self, non-self and detectors as bit-strings. The matching rule employed is the *r-contiguous bits matching rule*. Two bit-strings of equal length match under this rule if there exists a substring of length r at position p in each of them and these substrings are identical. Candidate detectors are produced using negative selection, i.e. they are created randomly and tested against the set of self strings. If they do not match any self string they become detectors. Similar to [2] we have collapsed different sorts of T- and B- cells (different types of detectors) into a single entity.

3.1 Experimental Setup

The goal of our experiments was to show what kind of impact misbehavior has on ad-hoc sensor networks and to what extent AIS are feasible for detection of such misbehavior. Therefore we used an ad-hoc scenario to simulate traffic within such a network.
Node distribution: Random way point snapshot of 1718 nodes in a square of $3km^2$.
Number of Connections: 10 connections with a constant bit rate of 1 packet per second.
MAC protocol: IEEE 802.11b.
Routing protocol: DSR.
Simulated time: 4 hours.
Hardware: Linux (SuSE 10.0) PENTIUM 4, 3GHz PC with 2 GB RAM.
Misbehavior: Dropping of packets which should be forwarded.

We produced two traffic trace files, one with normal behavior and one with misbehavior. Misbehavior was produced synthetically at 236 nodes. These nodes where programmed to drop 10% of all packets to be forwarded. From each trace file we produced 28 time windows each covering 500 seconds. We created antigens defined by genes for every node in a time window. Genes were created from the MAC and routing layer. We believe that combining several layers of the OSI model is necessary in order to generate invariant genes. We observed several values for every single time window: number of complete handshakes (RTS,CTS,DATA,ACK), number of RTS packets sent, number of data to be forwarded, number of data packets actually forwarded, average delay for each forward, number of RERR packets to be forwarded, number of RERR packets actually forwarded and its average delay. The last three values where taken from the routing layer, while the rest was taken from the MAC layer. The produced genes are the following:

Gene 1: $\frac{completeHandshakes}{numberOfRTSSent} \times 100$

Gene 2: $\frac{numberForwardedData}{numberDataToBeForwarded} \times 100$

Gene 3: Average delay between forwarding a data packet and forwarding at the next hop.

Gene 4: $\frac{numberRERRForwarded}{numberRERRToBeForwarded} \times 100$

Gene 5: Average delay between forwarding a RERR packet and forwarding at the next hop.

Each gene is a bit-string of length 10, where each bit represents an interval. Antigens were produced by concatenating the 5 genes. The undefined value of a gene was set to the maximum interval in case of genes 1, 2, 4 and to the minimum interval for genes 3 and 5.

We used an AIS with a *negative selection algorithm* and the *r-contiguous bits matching rule* for string matching (see also [3]) to detect misbehaviour for each node in all time windows.

4 Results

The experiments show that an AIS is able to detect misbehavior in an ad-hoc network using MAC and routing related genes as antigens. However the shifting of traffic[3] from a misbehaving area to an area where no traffic was present before, induced a mis-prediction anomaly. It is likely that this kind of mis-prediction would also occur on real nodes which encounter traffic for the first time. We produced two plots (see figure 1) showing the origin of misbehavior in the Ad-hoc scenario and the detection results by our AIS.

Picture at the top:
To produce a better to read plot only nodes with traffic ≥ 1000 packets are shown. Data was interpolated using the $pm3d$ function of gnuplot. The plot shows the misbehavior origin, i.e. the region of nodes which actually drop 10% of packets which should be forwarded.

Picture at the bottom:
The second picture shows the AIS detection results. Again the plots data was interpolated using the $pm3d$ function. All nodes which were detected by the AIS are used in the plot. The mentioned anomaly is the gray region on the left.

It seems that relying on the MAC and routing layer alone does not prevent mis-prediction at the moment. More genes combining the information of several OSI layers may be necessary.

We plan to extend our AIS in order to handle such anomalies. Furthermore we plan to test the effects of higher packet loss rates and other misbehavior scenarios (see [8], [10], [7]) with different numbers of nodes affected. We have therefore produced traffic traces for scenarios with 20%, 30% and 50% misbehavior.

In order to verify the simulation runs an implementation of a distributed Artificial Immune System on a sensor network[4] is mandatory.

References

[1] Zhou Ji, Dipankar Dasgupta. Real-Valued Negative Selection Algorithm with Variable-Sized Detectors. *Proc. Genetic and Evolutionary Computation Conference 2004 (GECCO-2004),* 2004: 287-298.

[2] S. Hofmeyr and S. Forrest. Immunity by Design: An Artificial Immune System. *Proc. Genetic and Evolutionary Computation Conference (GECCO)*, Morgan-Kaufmann, San Francisco, CA, pp. 1289-1296 (1999).

[3] Slaviša Sarafijanović and Jean-Yves Le Boudec. An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors. *Proc. ICARIS (Third international conference on artificial immune systems)*, 2004.

[4] Charles A. Janeway Jr. How the immune system works to protect the host from infection: a personal view. *Proc. Natl. Acad. Sci. U S A.*, 2001 Jun 19;98(13):7461-8.

[5] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod. Danger theory: The link between ais and ids. *Proc. International Conference on Artificial Immune Systems (ICARIS'03)*, pages 156–167, Edinburgh, UK, 2003.

[6] Uwe Aickelin, Julie Greensmith and Jamie Twycross. Immune System Approaches to Intrusion Detection - A Review. *Proc. the 3rd International Conference on Artificial Immune Systems (ICARIS 2004)*, Catania, Italy, 2004

[7] C. L. Barrett, M. Drozda, D. C. Engelhart, V. S. Anil Kumar, M. V. Marathe, M. M. Morin, S. S. Ravi, and J. P. Smith. Understanding Protocol Performance and Robustness of Ad Hoc Networks Through Structural Analysis. *Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005)*.

[8] Alvaro A. Cardenas, Svetlana Radosavac, John S. Baras. Detection and prevention of MAC layer misbehavior in ad hoc networks. *Proc. 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004.

[9] D'haeseleer, P., Forrest, S., and Helman, P. An immunological approach to change detection: Algorithms, analysis and implications. *Proc. IEEE Symposium on Research in Security and Privacy*, 1996.

[10] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. *Proc. ACM workshop on Wireless security*, 2003.

[3] DSR tries to find new routes between source and destination if a route becomes invalid.

[4] We will use Mica2 motes running *TinyOS*.

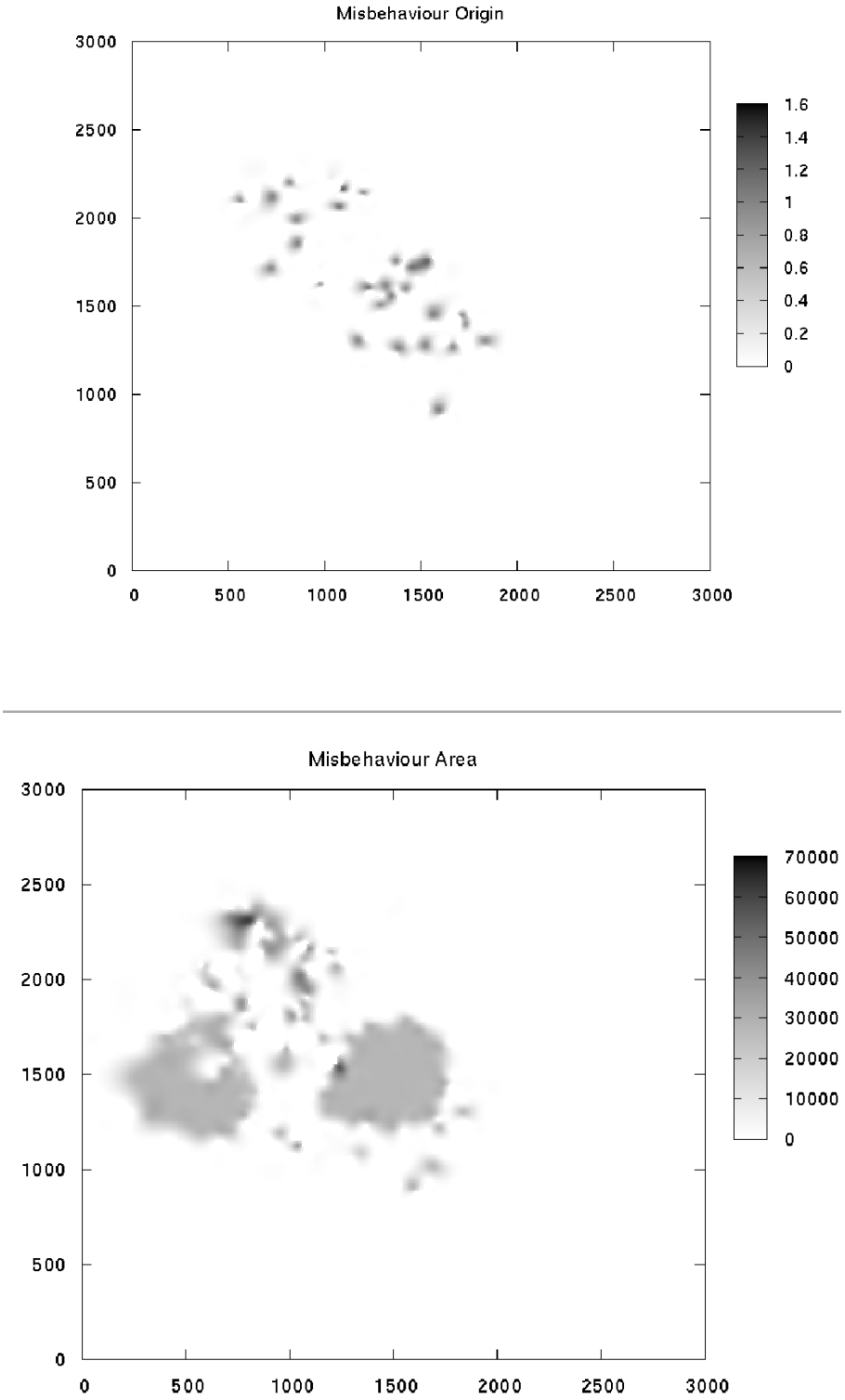

Figure 1: Misbehavior origin and the detection results from the AIS. Top picture only shows misbehaving nodes which have traffic $\geq$ 1000 packets. Bottom picture shows the detection results of the AIS. Both plots use interpolated data.