Securing Mobile Ad-Hoc Networks Using an Artificial Immune System

Ansgar Kellner
Institute of Computer Science
Göttingen, Germany
kellner@cs.uni-goettingen.de

Parisa Memarmoshrefi
Institute of Computer Science
Göttingen, Germany
memarmoshrefi@cs.uni-goettingen.de

Dieter Hogrefe
Institute of Computer Science
Göttingen, Germany
hogrefe@cs.uni-goettingen.de

ABSTRACT

Mobile Ad-hoc Networks (MANET) rely on the fundamental idea that all nodes act cooperatively to transfer data packets via multiple hops from a source to a remote destination. However, apart from the desired behaviour, in reality, malicious nodes can easily join the network and behave maliciously by not correctly participating in the network, e.g. by dropping packets or selectively forwarding packets. To mitigate the effect of malicious nodes in the network, in the first step, the misbehaving nodes must be identified. Based on the idea of biologically-inspired algorithms, in this paper, an artificial immune system is proposed that is able to detect misbehaving nodes in the network.

Categories and Subject Descriptors

C.2.0 [**Computer Systems Organization**]: Computer-Communication Networks—*Security and protection*

General Terms

Biologically-inspired Algorithms

Keywords

AIS, Artificial Immune Systems, MANET, Biologically-inspired Algorithms, Network Security

1. INTRODUCTION

A Mobile Ad-hoc Networks (MANET) is a distributed, autonomous system that consists of multiple mobile network nodes that communicate wirelessly with each other. Since no fixed infrastructure is involved the nodes must form an on-demand network with their surrounding network nodes. Due to their limited radio range the nodes must cooperate with each other to forward data packets via multiple hops from a source to a remote destination. However, the required cooperative behaviour of nodes can be exploited by malicious nodes that wants to save energy (selfishness) or just want to prevent the forwarding of data. Based on the idea of Sarafijanovic and Le Boudec[5] in this paper an artificial immune system (AIS) is proposed that is able to detect misbehaving nodes in a MANET.

The rest of the paper is organised as follows: in the second section of the paper the related work is discussed. Subsequently, in the third section, the idea of the artificial immune system is explained. The fourth section deals with the challenges of the work, while the fifth section summarises the work and gives an outlook for future work.

BICT 2014, December 01-03, Boston, United States

DOI 10.4108/icst.bict.2014.258086

2. RELATED WORK

Artificial Immune Systems (AIS), inspired by Human Immune Systems (HIS), are based on the idea that changes in the environment or deviations from normal behaviour can be detected in the complex systems.

Dressler et al. describe in their survey[2], how AIS can make use of HIS characteristics such as self-learning and memorisation. De Castro et al.[1] discuss three basic components of AIS that are often used: the representation of the system, affinity measures and adaption procedures. AIS are applied in different domains of problem solving, also in the realm of networking: Saleem et al.[4] propose the application of AIS in the area of network security for anomaly and misbehaviour detection in wireless sensor network routing. Sarafijanovic and Le Boudec[5] propose an AIS for misbehaviour detection in MANETs using the dynamic source routing protocol (DSR). A danger signal and memory detectors are introduced to increate the reliability of the AIS.

3. ARTIFICIAL IMMUNE SYSTEM

To solve the problem of detecting malicious nodes in the network an artificial immune system (AIS) is introduced, running on every node.

3.1 Artificial Immune System Architecture

The basic architecture of the AIS is depicted in figure 1. It consist of several building blocks that are interacting with each other.

In the *Mapping* block, the observed network traffic of the neighbouring nodes is recorded and mapped to antigens (see section 3.3).

The *Bone Marrow (BM)* block is responsible for the generation of new immature detectors, which are basically random bit strings of the same size as the antigens.

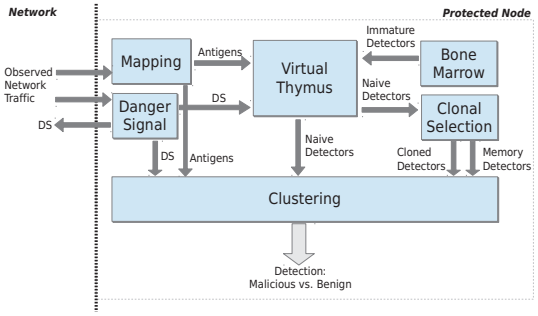

Figure 1: Artificial Immune System Architecture

The *Danger Signal (DS)* block deals with the creation and reception of danger signals. The DS are passed to the VT and the clustering block (see section 3.2).

The *Virtual Thymus (VT)* block is considered with the representation of 'self'. The VT continuously collects self-antigens by utilising the DS. The self-antigens are then used to negatively select the incoming immature detectors from BM.

The *Clonal Selection (CS)* block takes naive detectors from the VT, makes a copy of it and modifies this copy slightly. The original naive detector is passed as memory detector to the clustering block.

The *Clustering* block is responsible for deciding whether a neighbouring node is benign or malicious. The incoming antigens from the mapping block are checked against the naive detector (plus DS) and the memory detectors. When a certain threshold of matches is reached the clustering algorithm will be triggered to take the final decision.

3.2 Local Danger Signal

To reduce the number of false positives in the matching process Sarafijanovic and Le Boudec[5] introduced a Danger Signal (DS). For this work, this idea was seized and improved by introducing a local danger signal: when a node recognises a misbehaviour of another node, it sends a DS broadcast to its neighbours. A malicious node can only be detected when the naive detector matched and a DS for this time was received. An example is depicted in figure 2: since C does not

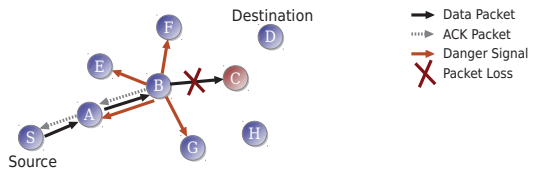

Figure 2: Propagation of the Danger Signal

send an ACK to B, B assumes that C is malicious and thus, B broadcasts this information to its neighbours.

3.3 Creation of Antigens

For the creation of antigens, each node observes the network traffic of its neighbours in radio range. The antigens are time-dependent, i.e. each antigen belongs to a certain time window ($\delta = 10s$). For a finer-grained resolution the time window is subdivided into a smaller parts ($\sigma = 10$).
In the first step, the observed network traffic is mapped to an intermediate format using the following labels:

`RREQ_SENT` (`A`), `RREP_SENT` (`B`), `RERR_SENT` (`C`), `DATA_SENT` (`D`), `RREQ_RECV` (`E`), `RREP_RECV` (`F`), `RERR_RECV` (`G`), `DATA_RECV` (`H`)

⇒ e.g. `EBEAFCHDHDHHHDEDHCHDDEA...`

Secondly, a set of *genes* is defined (regex) that are used to find patterns in the mapped traffic sequence. Each gene returns the number (#) of matches on the observed traffic sequence. The following genes are used:

G_1=#(E), G_2=#(E*(A|B)), G_3=#(H), G_4=#(H*D)
⇒ e.g. $(G_1, .., G_4) = (4, 3, 6, 3)$

Subsequently, the counted genes will be converted to a bit string, i.e. every time a defined gene counter threshold is exceeded in a σ part the bit will be set to 1. The final antigen for the time window δ can then be obtained by concatenating the obtained bit string parts, e.g.:

1111 0001 0000 0000 1010 0110 0000 0000 1111 1111

4. CHALLENGES

Though, the idea of the AIS seems to be straight forward, the implementation of the AIS leads to several challenges: as the number of possible antigens is quite high (2^{40}), the matching of detectors on antigens must be improved to reduce the required memory as well as the comparing runtime. As an idea the number of detectors could be reduced, but some sort of fuzzy matching could be applied instead.

5. SUMMARY AND OUTLOOK

In this paper, the use of an AIS in MANETs was investigated to detect malicious nodes in the network. The requirements and the resulting AIS has been explained. Currently, we are working on an implementation of the proposed AIS in OMNeT++[3] using fuzzy-matching for an optimised detection process. We hope to provide first results soon.

6. REFERENCES

[1] L. N. De Castro and J. Timmis. *Artificial immune systems: a new computational intelligence approach*. Springer, 2002.
[2] F. Dressler and O. B. Akan. A survey on bio-inspired networking. *Computer Networks*, 54(6):881–900, 2010.
[3] OMNeT++ Community. OMNeT++, Oct. 2014.
[4] K. Saleem, N. Fisal, S. H. S. Ariffin, S. K. S. Yusof, and R. A. Rashid. Biological inspired autonomously secure mechanism for wireless sensor networks. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, page 375, 2010.
[5] S. Sarafijanović and J.-Y. Le Boudec. An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal, and memory detectors. In *Artificial Immune Systems*, pages 342–356. Springer, 2004.