Mutual tests among agents in distributed intrusion detection systems using immunity-based diagnosis

Yuji Watanabe and Yoshiteru Ishida
Dept. of Knowledge-based Information Eng.
Toyohashi University of Technology
Toyohashi, Aichi 441-8580 JAPAN
watanabe@tutkie.tut.ac.jp and ishida@tutkie.tut.ac.jp

Abstract

Distributed intrusion detection systems have some advantages over centralized systems, such as scalability, resist subversion, and graceful degradation. With respect to resist subversion, however, self-monitoring is a difficult problem. One possibility is that each intrusion detection system is checked periodically by others.

In this paper, we propose mutual tests between intrusion detection system and mobile agent using immunity-based diagnosis. Some simulation results show that the credibility of normal intrusion detection system remains stable near 1, otherwise decreases to 0, and then corrupted ones are identified. Furthermore, we make sure that the diagnostic capability depends on some parameters.

Keywords: Intrusion detection system, Immunity-based diagnosis, Mobile agent, Self-monitoring

1 Introduction

The goal of intrusion detection is to identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators [1]. In the last few years, the need of intrusion detection system clearly increases with the growing number of network services, and then a large number of intrusion detection systems have been proposed (e.g., [2])

In order to design and build intrusion detection system, some researchers have drawn inspiration from the biological immune system. Forrest et al. have incorporated many properties of natural immune systems (distributed computation, error tolerance, adaptation and so on) into intrusion detection system [3, 4]. Spafford et al. also have developed the distributed intrusion detection system using autonomous agents regarded as immune cells [5, 6]. Mobile agents have been employed in intrusion detection system just as immune cells can circulate through the body [7, 8].

The intrusion detection systems inspired by the immune system are categorized into distributed system. Distributed intrusion detection systems have some advantages over centralized systems, such as *scalability, resist subversion*, and *graceful degradation* [6]. With respect to *resist subversion*, however, *self-monitoring* is a difficult problem. In other words, corrupted intrusion detection system cannot identify illegitimate use correctly; therefore it is necessary to discern which ones can be faulty. Although Spafford et al. suggested one possibility with each monitoring agent being checked periodically by several others, they achieved no detailed examination [6].

In this paper, we propose mutual tests using an *immunity-based diagnosis* in distributed intrusion detection system. The original immunity-based diagnostic model has been proposed by Ishida who is one of authors [9, 10]. The immune system can be considered as fully distributed diagnosis, where a large number of immune cells detect and eliminate non-self by stimulating and suppressing other cells. The diagnosis is performed by mutual tests among units and dynamic propagation of active state.

Furthermore, mobile agents contribute to the mutual tests in the diagnosis. In conventional approaches [7, 8], mobile agents directly monitor host computers, while mobile agents in our method observe intrusion detection systems. Our mobile agent acts as an additional module for existing intrusion detection systems.

To verify the feasibility of our diagnosis, we carry out some simulations. The result shows that the credibility of normal intrusion detection system remains stable near 1, otherwise decreases to 0, and then corrupted ones are determined. In addition, we execute the diagnosis changing two parameters: number of mobile agents and number of intrusion detection system's rules. We confirm what effects these parameters have on the diagnostic capability.

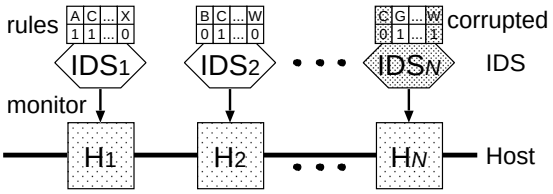

Figure 1: Simulated distributed intrusion detection system.

2 Distributed intrusion detection system with mobile agents

2.1 Simulated intrusion detection system

For easy performance analyses, the immunity-based diagnosis is applied to a simulated distributed intrusion detection system. Figure 1 illustrates the simulated system, where N intrusion detection systems can monitor the corresponding host computer using some rules. Real intrusion detection systems as show in Fig. 2 possess a lot of complicated rules, which are collected in some files according to service (for example, *dns.rules* file corresponding to DNS service). The rules are simplified by a pair of label (A, B, C, $\cdots$) and data (0 or 1). The total number of rules is defined by L, and each intrusion detection system has $L_h(\leq L)$ rules on average because each host provides different service. If $L_h = L$, then distributed intrusion detection system become homogeneous, otherwise heterogeneous.

We suppose that corrupted intrusion detection system includes some wrong rules represented by inversion of data (0 or 1). In Fig.1, although C:1 and W:0 are correct pairs, the corrupted intrusion detection system IDS_N has two inverted rules. Each simulation starts with the condition where there are $N_f(\leq N)$ corrupted intrusion detection systems.

2.2 Mobile agent

Each mobile agent with a piece of rules can migrate from host to host in order to check intrusion detection system mutually as depicted in Fig.3. The average number of agent's rules is represented by $L_a(\leq L)$. We assume that there are checks among agents on the same host (e.g., Ma_1 and Ma_2), while there is no test among hosts (e.g., IDS_1 and IDS_2) because mobile agent exists on behalf of communication between hosts. We will explain a concrete test outcome in **3.2**.

At the beginning of simulation, each intrusion detection system creates some mobile agents by duplicating a part of the rules. As a result, normal intrusion detection system bears fault-free mobile agents, while corrupted intrusion detection system has faulty mobile

```
[root@wata root]# ls /etc/snort/
RCS                         local.rules        snmp.rules
attack-responses.rules      misc.rules         snort.conf
backdoor.rules              multimedia.rules   snort_tutkie.conf
bad-traffic.rules           mysql.rules        sql.rules
chat.rules                  netbios.rules      telnet.rules
classification.config       nntp.rules         tftp.rules
ddos.rules                  oracle.rules       virus.rules
deleted.rules               other-ids.rules    web-attacks.rules
dns.rules                   p2p.rules          web-cgi.rules
dos.rules                   policy.rules       web-client.rules
experimental.rules          pop3.rules         web-coldfusion.rules
exploit.rules               porn.rules         web-frontpage.rules
finger.rules                reference.config   web-iis.rules
ftp.rules                   rpc.rules          web-misc.rules
icmp-info.rules             rservices.rules    web-php.rules
icmp.rules                  scan.rules         x11.rules
imap.rules                  shellcode.rules
info.rules                  smtp.rules
[root@wata root]# head /etc/snort/web-cgi.rules
# (C) Copyright 2001,2002, Martin Roesch, Brian Caswell, et al.
#    All rights reserved.
# $Id: web-cgi.rules,v 1.56 2002/08/18 20:28:43 cazz Exp $
#--------------
# WEB-CGI RULES
#--------------
#

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-CGI
HyperSeek hsx.cgi directory traversal attempt"; uricontent:"/hsx.cgi";
content:"../../"; content:"%00"; flow:to_server,established;
reference:bugtraq,2314; reference:cve,CAN-2001-0253;
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-CGI
HyperSeek hsx.cgi access"; uricontent:"/hsx.cgi"; flow:to_server,
established; reference:bugtraq,2314; reference:cve,CAN-2001-0253;
classtype:web-application-activity; sid:1607;  rev:3;)
[root@wata root]#
```

Figure 2: Example of snort rules [2].

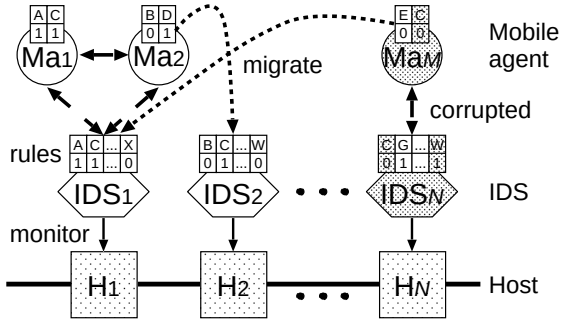

Figure 3: Mutual tests using mobile agents.

agents with some inverted rules (for example, Ma_M in Fig.3). Note that false mobile agents misdiagnose normal intrusion detection system.

3 Immunity-based diagnosis

3.1 Distributed diagnosis model

The distributed diagnosis models inspired by the biological immune system have been proposed by Ishida [9, 10]. The distributed diagnosis is performed by mutual tests among units and dynamic propagation of active states. In the model, each unit has the capability of testing other units, and being tested by the others as well. A state variable R_i indicating the *credibility of unit* is assigned to each unit and calculated as follows:

$$\frac{dr_i(t)}{dt} = \sum_j T_{ji}R_j + \sum_j T_{ij}R_j - \frac{1}{2}\sum_{j\in\{k:T_{ik}\neq 0\}}(T_{ij}+1), \tag{1}$$

$$R_i(t) = \frac{1}{1 + \exp(-r_i(t))}, \tag{2}$$

where the credibility $R_i \in [0, 1]$ is a normalization of $r_i \in (-\infty, \infty)$ using a sigmoid function. In equation (1), T_{ij} denotes binary test outcome from unit i to j as defined in **3.2**.

The diagnosis represented by the differential equation (1) has two characteristics. First, the credibility of tested unit i is updated by the sum of *the test value weighted* by the credibility of testing unit j. The weighted test value leads to neglect the test outcome of false unit with low credibility. Secondly, the credibility of unit i is evaluated not only from the opinions of other testing units, but also from the opinions of what the unit said to the other units. The former corresponds to the first term of the right-hand side of equation (1), and the latter to the second and third term. We call the latter *reflection effect*. The reflection effect is somewhat similar to the situation that if you criticize a highly respected person, it affects your own credit.

3.2 Test outcome

We explain how units, namely, both IDS and mobile agent, can produce their test outputs. The test outcome is assigned to -1, 0 or 1 according as whether or not rules are the same:

$$T_{ji} = \begin{cases} 1 & \text{if all rules match} \\ -1 & \text{if one or more mismatches exist} \\ 0 & \text{if all rules are not comparable} \\ -1/0/1 & \text{if unit } j \text{ is abnormal} \end{cases}. \tag{3}$$

For example, in Fig. 3, the test outcome between Ma_1 and IDS_1 becomes 1 with the agreement of both rules A and C, the output between Ma_2 and IDS_1 is 0 because Ma_2 rules are not comparable with IDS_1 ones, and corrupted Ma_M and IDS_N replay unstably.

4 Simulation

4.1 False positive and false negative

The feasibility of the immunity-based diagnosis is verified by some simulations. In each simulation step, we record not only the credibility of intrusion detection system but also two evaluation indexes, that is, *false positive rate* α and *false negative rate* β as follows:

$$\alpha = \frac{N_t^{low}}{N - N_f}, \tag{4}$$

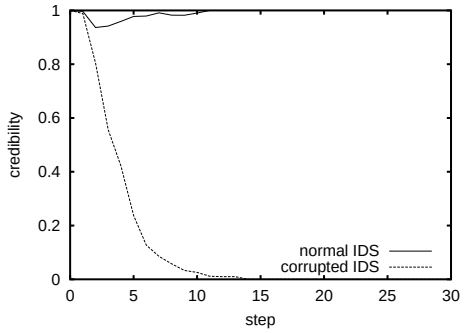

Figure 4: Transition of the average credibility R_i for normal and corrupted IDS over 50 trials.

Table 1: Parameters list.

	Description of variable
$R_i(0)$	Initial value of credibility
$r_i(0)$	Initial value of intermediate variable
N	Number of IDSs (hosts)
N_f	Number of corrupted IDSs
M	Number of mobile agents
L	Total number of rules
L_h	Average number of IDS's rules
L_a	Average number of agent's rules

$$\beta = \frac{N_f^{high}}{N_f}, \tag{5}$$

where $N - N_f$ denotes the number of normal intrusion detection systems, and N_f the number of corrupted ones. N_t^{low} is the number of normal intrusion detection systems with the credibility of not more than 0.8 ($R_i \leq 0.8$), while N_f^{high} is the number of corrupted intrusion detection systems with the credibility of not less than 0.2 ($R_i \geq 0.2$). The false positive means that the diagnosis regards normal as abnormal, while the false negative results from identifying abnormal as normal.

4.2 Results

Figure 4 illustrates transition of the average credibility for normal and corrupted intrusion detection system over 50 trials. In this simulation, the parameters listed in Table 1 are fixed: $R_i(0) = 1.0$, $r_i(0) = 1.0$, $N = 50$, $N_f = 50$, $M = 300$, $L = 5000$, $L_h = 500$ and $L_a = 50$. The result shows that the credibility of normal intrusion detection system remains stable near 1, otherwise decreases to 0, and then corrupted one is determined.

Other simulations are carried out with changes of two parameters, that is, the number of mobile agents

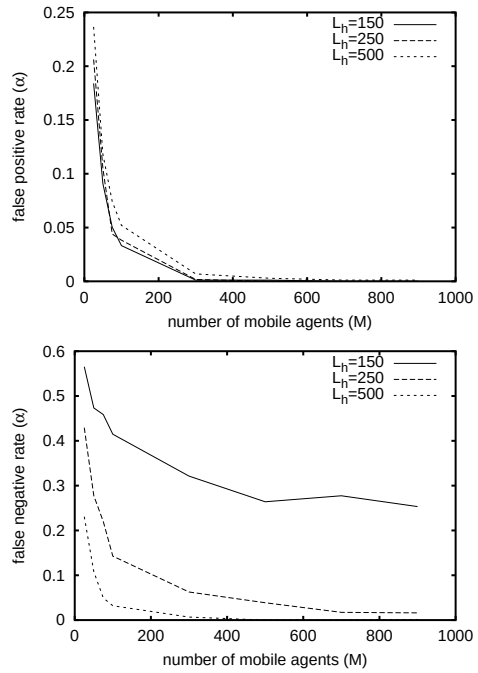

Figure 5: Average false positive/negative rate (α and β) vs. number of mobile agents (M).

(M) and the average number of intrusion detection system's rules (L_h). Figure 5 presents average false positive rate and false negative rate after 30 steps over 50 trials, changing M and L_h. From these results, by the more mobile agents an intrusion detection system is mutually tested, the more precisely its credibility can be calculated. In terms of L_h, the more common rules all intrusion detection systems have, namely, the more homogeneous all intrusion detection systems become, the more easily corrupted ones will be detectable.

These results also demonstrate that the false negative rate β tends to be inferior to the false positive rate α. The reason is probably that some corrupted agent that a corrupted intrusion detection system produces as alter ego at the beginning of simulation can increase the credibility of the parental corrupted intrusion detection system. We conclude that these parameters have important effects on the diagnostic capability.

5 Conclusions and further work

In this paper, we proposed mutual tests between intrusion detection system and mobile agent using the immunity-based diagnosis. The result shows that the credibility of normal intrusion detection system remains stable near 1, otherwise decreases to 0, and then corrupted ones are identified. Furthermore, we confirm that the diagnostic capability depends on both the number of mobile agents and the number of intrusion detection system's rules.

In further work, we will examine the diagnostic capability in more detail and incorporate the immunity-based diagnosis to a real distributed intrusion detection system.

Acknowledgements

This research has been supported in part by International Communications Foundation.

References

[1] B. Mukherjee, L. T. Heberlein, and K. N. Levitt (1994), Network intrusion detection. *IEEE Network*, 8(3), pp. 26–41

[2] Snort.org. http://www.snort.org/.

[3] S. Forrest, S. Hofmeyr, A. Somayaji, and T. Longstaff (1996), A sense of self for unix process. In *Proc. of 1996 IEEE Symposium on Security and Privacy*, pp. 120–128

[4] S. Hofmeyr and S. Forrest (2000), Architecture for an artificial immune system. *Evolutionary Computation Journal*, 7(1), pp. 45–68

[5] M. Crosbie and E. Spafford (1995), Defending a computer system using autonomous agents. In *Proc. of the 18th National Information Systems Security Conference*

[6] E. Spafford and D. Zamboni (2000), Intrusion detection using autonomous agents. *Computer Networks*, 34, pp. 547–570

[7] G. Helmer, J. Wong, V. Honavar, and L. Miller (1998), Intelligent agents for intrusion detection. In *Proc. of the IEEE Information Technology Conference*, pp. 121–124

[8] D. Dasgupta (1999), Immunity-based intrusion detection systems: a general framework. In *Proc. of the 22nd National Information Systems Security Conference*, pp. 18–21

[9] Y. Ishida (1990), Fully distributed diagnosis by PDP learning algorithm: towards immune network PDP model. In *Proc. International Joint Conference on Neural Networks*, pp. 777–782

[10] Y. Ishida (1996), An immune network approach to sensor-based diagnosis by self-organization. In *Complex Systems*, 10, pp. 73–90