한국시뮬레이션학회 논문지
Vol. 16, No. 1, pp. 59-68 (2007. 3)

필수 서비스의 침입감내를 위한 그룹관리 프로토콜의 신뢰성 분석

김형종[1†] · 이태진[2]

A Dependability Analysis of the Group Management Protocol for Intrusion Tolerance of Essential Service

Hyung-Jong Kim · Tai-Jin Lee

ABSTRACT

IT (Intrusion Tolerant) technology is for guaranteeing the availability of service for certain amount time against the attacks which couldn't be prevented by the currently deployed information security countermeasures. IT (Intrusion Tolerant) technology mainly makes use of the replication of service and system for enhancing availability, and voting scheme and GMP (Group Management Protocol) are used for the correctness of service. This paper presents a scheme to analyze dependability of IT (Intrusion Tolerant) technology through probabilistic and simulation method. Using suggested analysis scheme, we can analyze the robustness and make a sensible trade-offs in of IT (Intrusion Tolerant) technology.

Key words : Dependability, Group management, Voting, Intrusion tolerance system, Availability

요 약

침입감내 기술은 기존의 정보보호 기술이 방어하지 못하는 공격들이 있는 상황에서 일정 시간 동안 일정 수준의 서비스 품질을 유지시키기 위해 사용되는 기술을 일컫는 말이다. 침입감내 기술을 통해서, 서비스 혹은 이를 제공하는 시스템의 가용성 및 신뢰성을 높여 줄 수 있고, 공격으로 인한 피해를 줄일 수 있게 된다. 침입감내 기술의 핵심 기술 중 하나가 그룹관리 프로토콜 (GMP : Group Management Protocol) 및 투표 기능(Voting) 이다. 본 논문은 이 두 요소기술이 갖는 신뢰성을 수학적으로 검증하고 또한, 시뮬레이션을 통한 검증을 수행하였다. 이러한 분석이 갖는 의미는, 분석 결과를 활용한 보안 정책을 만들 수 있다는 것과, 다수개의 시스템의 결과를 기반으로 의사결정을 해야 하는 경우에 어떠한 분석 절차를 가져야 하는 지에 대한 방법론을 제시한다는 것이다.

주요어 : 의존성, 그룹 관리, 투표, 침입감내 시스템, 가용성

1. Introduction

In the security research area, the survivability related work is urgently required to preserve the continuity of essential services such as DNS, DHCP and so on. One of those works is the ITS (Intrusion Tolerant System) which enables client users to access the service though severe attack is occurred. One of the fundamental component of ITS is the group manager. It performs voting, leader selection, configuration and management. In many related projects, the performance of group management has been analyzed and simulated but the dependability hasn't been analyzed.

In our work, we analyze the dependability of the group management theoretically and validate the result using simulation. Especially, the method of analyzing dependability is applicable to the systems which are composed of the untrusting nodes. Through simulation result, we have a good reference to setup the security management policy in our ITS because we are able to

* 이 논문은 2007학년도 서울여자대학교 교내특별과제연구비의 지원을 받았음.

2007년 3월 21일 접수, 2007년 3월 26일 채택

[1] 서울여자대학교 컴퓨터학부
[2] 한국정보보호진흥원 IT인프라보호단
주 저 자 : 김형종
E-mail; hkim@swu.ac.kr

figure out the relation between the cost and dependability.

In this paper, we introduce the group management scheme in ITS and analyze its dependability theoretically. At the second section, we show the projects related to the intrusion tolerant technology, their aims and properties. The third section shows analyzing method theoretically about the majority voting and corrupt member detection dependability. The fourth section shows the dependability of the group management and validates it according to the several factors. The fifth section presents the dependability matrix and conclusions.

2. Related Work

Among the ITS related work, MAFTIA[1,2] is representative research project which is conducted by EU's IST. MAFTIA's principle about the intrusion is that all intrusion cannot be protected and some of them should be allowed to be in a system, and system must prepare something about those attacks. Based on this principle, middleware-like ITS framework which contains five main modules is suggested. The five main components are intrusion detection module, group communication protocol, encryption module, data fragmentation/scattering, and user access control.

The OASIS project[3,4,6,7,8] that is conducted by DARPA proceeds 12 research projects which are categorized four research topics such as server architecture, application program, middleware, network fundamental technology. There are main concepts of the 12 project in OASIS should consider as principles in their project. First, the diversity of application and OS platform enhances the availability of the service and system because usually the intrusions exploit vulnerabilities that exist in a specific system platform. Second, the system and service should be redundant and if there is intrusion or fault that causes problem in system or service, the redundant system or service do the work of main system and service during the restoring time. Third, there are some mechanisms to guarantee the integrity and availability of services, and those mechanisms cooperate with the security mechanisms such as intrusion prevention and detection. To enhance the availability, load-balancing facility is applied and to enhance the integrity of service, voting mechanism, service member isolation and restoration are used. The Fourth there are monitoring facility that used to see the abnormal status of services and systems. In the tolerant system, as the monitoring is done after the prevention and detection mechanism is applied, the monitoring factor selection is should be specialized.

3. Dependability Analysis with the theoretical method

3.1 Background

Intrusion tolerance technology should consider the two main aspects such as of FT (Fault Tolerance) and security. As for fault tolerance technology, redundancy, diversity, dynamic reconfiguration and voting should be considered. Also, to assure the availability and correctness, those FT technologies are used in group manager in FT technology. As for the security technology, the intrusion detection and prevention are accepted as core functions. In this paper, we are supposed to analyze the dependability of the group management, because its dependability is related to that of the intrusion tolerant technology.

Group management technology is composed of corrupt detector, leader selector, voter, group information manager. The corrupt detector looks for the corrupt members in the group and leader selector assorts the leader, where the leader is corrupted or should be changed manually. The voter selects the adequate service response from the ones received from all members, and group information manager performs adding or deleting of members in the group. These components are very important in group management. Since they are triggered by the corrupt detector, if the corrupt detection does not operate correctly, the other components cannot perform their own functions well.

So it is important to analyze the dependability of the corrupt detection.

There are several corrupt detection mechanisms, but they can be simplified as essential common steps as shown in below.

1) The leader multicasts the heartbeat to all the other members of the group periodically. Heartbeat simply means the message to check its availability, and demands the member's resource states or the response.
2) Each member sends the adequate response to the leader according to the leader's heartbeat. Since each member also cannot trust the leader, they examine the leader's state periodically.
3) The leader collects all the responses and determines whether the members of the group are corrupted or not. If the leader detects the corrupt member, it can trigger the group information manager to delete corrupted member from the group or analyze the corrupted member in detail or alarm to the SSO (Site Security Officier).

To analyze the dependability of the corrupt detection mechanism, we extract the following parameters.

n : the number of members belong to the group
m : the number that the group can regard the group decision as correct response.
p : the probability that the member is corrupted.
r : the probability that the member can detect the corrupted member correctly.
s : the probability that the member regards the correct member as the corrupt member.

In this section, we analyze majority voting and the dependability of the corrupt detection in the group management conceptually.

3.2 Analysis of the Majority Voting

In the intrusion tolerant system, there are many replicated members and we have to manage these members to accomplish the required functionality. In order to extract the correct decision from the responses of the members for the client's request and manage these members, we basically need to have voting and group management mechanisms. Voting has the various mechanisms and in this paper we deal with the majority voting, which means that we regard the major responses as the correct result.

- Definition

corrupt : the state that the member cannot extract the right response from the client's request
correct : the state that the member can extract the right response from the client's request

P(condition, result, number)

Condition (Correct or Incorrect) : whether the originally correct response matches the response from voter or not
Result (Select or Not Select) : whether the voter can extract the result or not
Number : the number that the group can regard the group decision as correct response. In other words, if the number of the same response is bigger than this number the response is selected by voter.

Although voter can extract more dependable result than single member's service, it does not mean the correct result. Now we analyze the dependability of the voting. We can think of three cases.

- P(Correct, Select, m) : the probability that the number of the correct members is higher or equal than m. It means that voter extracts the correct result and originally correct.
- P(Incorrect, Select, m) : the probability that the number of the corrupt members is higher or equal than m. It means that voter extracts the correct result but originally not correct.
- P(Incorrect, Not Select, m) : the probability that the number of all the members which have the same responses is smaller than m. It means that

voter cannot extract the correct result

- property

P(Correct, Select, m) + P(Incorrect, Select, m) + P(Incorrect, Not Select) = 1

P(Correct, Select, m) + P(Incorrect, Select, m) : The probability that voter regards as the correct result.

P(Incorrect, Not Select, m) : It means that voter cannot extract the result. Since we know that the voter cannot extract the result, we can trigger server events and react in many ways.

The problem happens that when the voter regards it as the correct result but originally not correct. We define it as Voting Failure Rate. P(Incorrect, Select, m) means Voting Failure Rate. So we will calculate it.

◆ Calculation

in case of the number of the correct members >= m,

$$P(Correct, Select, m) = \sum_{k=m}^{n} {}_nC_k(1-p)^k p^{n-k}$$

Before we calculate the P(Incorrect, Select, m), we define the term c. The corrupt members may get the arbitrary responses and some of them get the same responses. If the number of the same corrupt responses is higher or equal than m, the voter regards the wrong responses as the correct one. The portion of the largest group which respond corruptly is defined as c, and we can calculate the P(Incorrect, Select, m) using c.

- Definition

$p_k(\in correct, Select, m)$

In case that the number of the corrupt members is k, it means the probability that the voter extracts wrong responses.

$$P_n(\in correct, Select, m)$$
$$= {}_nC_n(1-p)^0 p^n \times (\sum_{k=m}^{n} {}_nC_k(1-c)^{n-k}c^k)$$

$$P(\in correct, Select, m) = \sum_{k=m}^{n} P_k(\in correct, Select, m)$$

Therefore,

$$P(\in correct, Select, m)$$
$$= \sum_{k=m}^{n} [{}_nC_k(1-p)^{n-k}p^k \times (\sum_{s=m}^{k} {}_kC_s(1-c)^{k-s}c^s)]$$

P(Incorrect, Not Select, m) = 1 - P(Correct, Select, m) - P(Incorrect, Select, m)

◆ Result

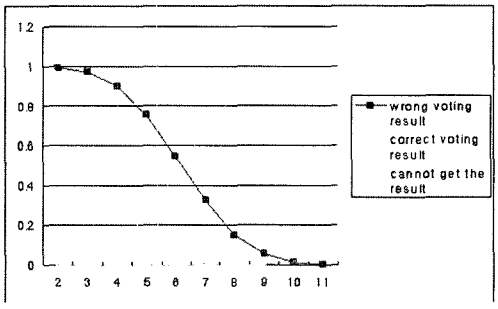

figure 1. Dependability Graph according to m

If m increases, the probability of the correct result increases, and if m decreases, the probability of the correct result decreases. However, if m is more than 10, voting rule is so strict that the probability of the correct voting decreases, and the probability which voter cannot extract the correct result increases.

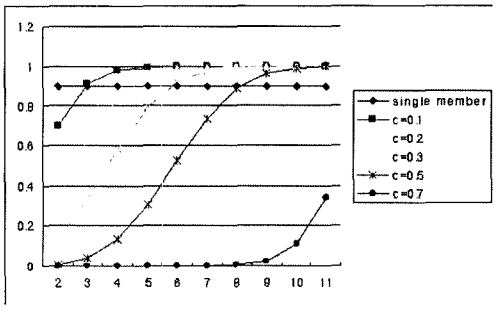

figure 2. Replicated members vs single member

The dependability of the single member is 0.9, if we use the voting through the replicated members, we must ensure dependability higher than that of the single member. According to the graph, in case of c=0.1 and m=4, the dependability is up to 0.99. However if c is up to 0.5, the dependability using the voting is very low and useless. The c means the measurement whether

the member is corrupted or not when the same attacks occur in the same time. Through this graph, we can determine clearly whether the voting can enhance the dependability or not for the particular system.

3.3 Analysis of the Member Detection

As we mentioned previously, each group member sees if the other members are corrupted periodically. Now we analyze the dependability of the corrupt member detection more theoretically.

◆ Member Detection by each member

- Definition

$D_{corrupt}$: the probability that the arbitrary member A regards the arbitrary member B as the corrupt member

$D_{correct}$: the probability that the arbitrary member A regards the arbitrary member B as the correct member

When a member detects the state of the other member, there are several cases.

Table 1. Member Detection by each member

		Real state of the detected member	
		Correct	Corrupt
Real state of the detecting member	Correct	Correct decision (D4) [Correct Result]	Corrupt decision (D1) [Correct Result]
		Corrupt decision (D3) [Incorrect Result]	Correct decision(D2) [Incorrect Result]
	Corrupt	Correct decision (D6) [Correct Result]	Correct decision (D8) [Incorrect Result]

Probability of the D1 : (1 - p) p r

Probability of the D2 : (1 - p) p (1 -r)

Probability of the D3 : (1 - p) (1 - p) s

Probability of the D4 : (1 - p) (1 - p) (1 -s)

Probability of the D6 : p (1 - p)

Probability of the D8 : p p

$D_{corrupt}$ = D1 + D3

$D_{correct}$ = D2 + D4 + D6 + D8

when member A regards member B as corrupt, the probability of the correct decision = $\frac{D1}{D_{corrupt}}$

when member A regards member B as corrupt, the probability of the incorrect decision = $\frac{D3}{D_{corrupt}}$

when member A regards member B as correct, the probability of the correct decision = $\frac{D4+D6}{D_{corrupt}}$

when member A regards member B as correct, the probability of the correct decision = $\frac{D2+D8}{D_{corrupt}}$

◆ Group Member Detection by all members in group

When n-1 members detect the state of the arbitrary member A, there are four cases.

Table 2. Member Detection by whole group

		Detection Result of the member A	
		Corrupt (greater or equal than m)	Correct (less than m)
Real state of the member A	Corrupt	(P1) member A Corrupt	(P2) Member A Corrupt
	Correct	(P3) member A Correct	(P4) member A Correct

P1 + P2 + P3 + P4 = 1

$$P1+P3=\sum_{k=m}^{n-1} {}_{n-1}C_k D_{corrupt}^{\ k} D_{correct}^{\ n-1-k}$$

So if we calculate P1, we can calculate the other probabilities.

- Definition

P(t) : the probability that t members regard the corrupted member as the corrupt

P(t, m) : in P(t), the probability that the number of the correct detection members is greater or equal than m

$$P(t) = {}_{n-1}C_t D_{corrupt}^{\ t} D_{correct}^{\ n-1-k}$$

P(t, m) = 0

where, 0 <= i < m, n-1-t < m- i

$$P(t,m) = \sum_{i=0}^{t} {}_tC_i \left(\frac{D1}{D_{corrupt}}\right)^i \left(\frac{D3}{D_{corrupt}}\right)^{t-i}$$
$$\left[\sum_{j=m-i}^{n-1-t} {}_{n-1-t}C_j \left(\frac{D2+D8}{D_{correct}}\right)^j \left(\frac{D4+D6}{D_{correct}}\right)^{n-1-t-j}\right]$$

where, 0 <= i < m, n-1-t >= m- i

$$P(t,m) = \sum_{i=0}^{t} {}_tC_i \left(\frac{D1}{D_{corrupt}}\right)^i \left(\frac{D3}{D_{cprrupt}}\right)^{t-i}$$

where, m < i

$$P1 = \sum_{t=m}^{n-1} P(t)P(t,m)$$

Using above expression, we can calculate P1, P2, P3 and P4.

4. Simulation-based Dependability Analysis

In the previous chapter, we present the theoretical analysis for dependability of group management scheme. From now on, we will validate the method using data in intrusion tolerance.

4.1 Simulation Overview

When we see one corrupt member detection as one unit, one unit means

- Group can extract the detection result about the states of all the members
- One unit performs n n-1 detection times
- Before one unit starts, corrupted members exist arbitrary in the probability of p and after one unit, we can extract detection result.
- So we can extract the dependability from one unit.
- Each unit is independent

Detection of each member can be classified as four cases

Table 3. Member Detection by each Member

Real state of the member A	Detection result about member B	meaning
Corrupt	Corrupt	Correct Detection for a corrupt member (S1)
	Correct	Incorrect Detection for a corrupt member (S2)
Correct	Corrupt	Incorrect Detection for a correct member (S3)
	Correct	Correct Detection for a correct member (S4)

When arbitrary member A detects arbitrary member B, member A decides one of the four cases. This shows that arbitrary one member detects arbitrary one member. Since n-1 members detect the arbitrary member, we need to extract the result by all member of group.

Table 4. Member Detection by whole group

Real state of the member A	Detection result by each member	number	meaning
Corrupt	Corrupt	n1 (number of S1)	if n1>= m, correct detect (G1)
	Correct	n2 (number of S2)	if n2>= m, false negative (G2)
Correct	Corrupt	n3 (number of S3)	if n3>= m, false positive (G3)
	Correct	n4 (number of S4)	if n4>= m, correct detect(G4)

For the arbitrary member, n-1 members get the result among S1, S2, S3, S4. If the number of each n1~n4 is greater or equal than m, we regards it as the group decision. Additionally, if member A is corrupt, group decision is G1 or G2 and if member A is correct, group decision is G3 or G4. If group extracts G1, G2 or G3,

G4, we decide those as G2, G3 respectively, because it is not correct detection.

This procedure applies to arbitrary member A. Since all the members need to extract the detection result, we repeat it n times. So G1 + G2 + G3 + G4 = n and G1, G4 means the number of the correct detection. G2 means the number of the false negative detection and G3 means the number of the false positive detection. Since this number is proportional to the n, we can represent the dependability as below.

The probability of the false negative detection : $\frac{G2}{n}$

The probability of the false positive detection : $\frac{G3}{n}$

The probability of the correct detection : $\frac{G1+G4}{n}$

We repeat the unit 1000 times according to each situation and extract the simulation result. In the next section, we will show the result.

4.2 Dependability Analysis of the Member Detection with Tolerance Respect

In the particular intrusion tolerant system, p is the fixed value and n, m can be changeable according to the security policy. m means the standard which extracts the group decision. As m changes, false negative detection and false positive detection rates are changeable sensitively. So it is important to find a adequate m.

- Dependability Analysis as a function of m

Table 5. Detection Error according to m

m	False positive detection rate	False negative detection rate
3	15.033333%	0.000000%
4	3.700000%	0.000000%
5	0.625000%	0.008333%
6	0.066667%	0.191667%
7	0.000000%	0.783333%
8	0.000000%	2.625000%
9	0.000000%	5.800000%
10	0.000000%	11.383333%

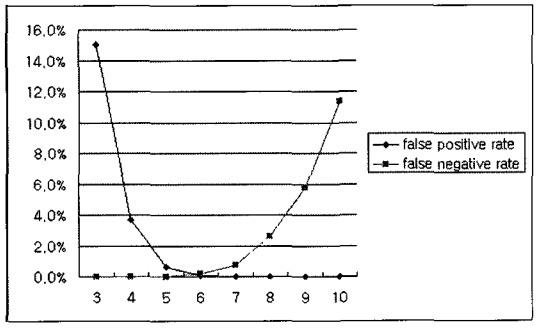

figure 3. Detection Error according to m

As m increases, false positive detection rate decreases and false negative detection rate increases. Because false negative detection means that the group allows the corrupt member, false negative detection rate must be 0 or very low. However, false positive detection generates only some overhead. That is, false positive detection is not directly related to the dependability. According to the two requirements, the most adequate m is 4. In other words, m means $\frac{n}{3}$ considering the proportion between n and m.

- Dependability Analysis as the function of p

Table 6. Detection Error according to p

p	False positive rate	False negative rate
0.0001	9.308333%	0.000000%
0.001	9.150000%	0.000000%
0.01	9.575000%	0.000000%
0.05	7.791667%	0.000000%
0.1	6.533333%	0.000000%
0.2	3.300000%	0.000000%
0.3	1.916667%	0.008333%
0.4	1.100000%	0.425000%

As p increases, false positive detection rate decreases and false negative detection rate increases. And as p approaches to 0, false positive detection goes to s. As you see, false positive detection rate and false negative detection rate cannot be changed by p to some extent. So p is not the critical factor to analyze the dependability of the group management.

4.3 Dependability Analysis of the Member Detection with Security Respect

In the previous section, we analyze the dependability about majority standard m, corrupt rate p. Since it is based on corrupt member detection, the dependability from n, m is very changeable according to various detection mechanisms. So we analyze the dependability for various detection mechanisms.

- Dependability Analysis as a function of r

Table 7. Detection Error according to r

r	FP (p=0.1)	FN (p=0.1)	FP (p=0.2)	FN (p=0.2)	FP (p=0.3)	FN (p=0.3)
0.5	5.925000%	0.216667%	3.116667%	0.958333%	2.091667%	3.008333%
0.6	5.958333%	0.016667%	3.175000%	0.383333%	2.208333%	1.475000%
0.7	6.075000%	0.000000%	3.433333%	0.125000%	2.258333%	0.483333%
0.8	5.800000%	0.000000%	3.450000%	0.016667%	2.041667%	0.166667%
0.9	5.641667%	0.000000%	3.483333%	0.008333%	1.900000%	0.041667%

False positive detection rate : FP
False negative detection rate : FN

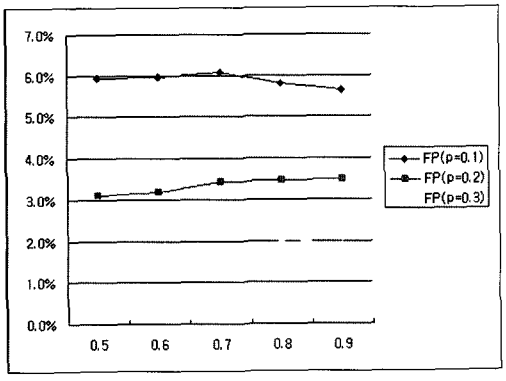

figure 4. false positive rate according to r

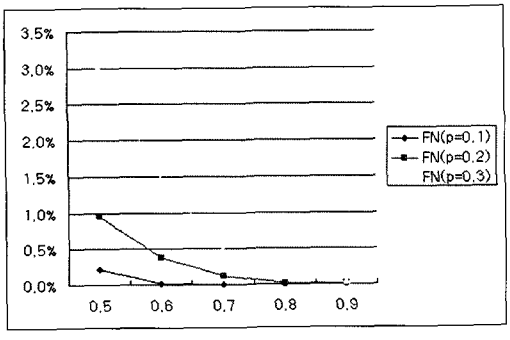

figure 5. false negative rate according to s

As r increases, false positive detection rate does not change and false negative detection rate decreases gradually. Since false positive detection rate has nothing to do with r and generates only overhead. However, as r decreases, false negative detection rate highly decreases.

- Dependability Analysis as a function of s

Table 8. Detection Error according to s

s	FP (p=0.1)	FN (p=0.1)	FP (p=0.2)	FN (p=0.2)
0.1	6.133333%	0.000000%	3.783333%	0.000000%
0.2	26.925000%	0.000000%	17.566667%	0.000000%
0.3	52.450000%	0.000000%	37.683333%	0.000000%
0.4	73.116667%	0.000000%	56.833333%	0.000000%
0.5	82.741667%	0.000000%	68.283333%	0.000000%

False positive detection rate : FP
False negative detection rate : FN

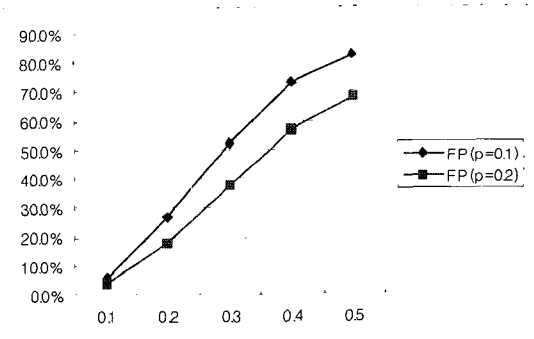

figure 6. false positive rate according to s

As s increases, false positive detection rate highly increases and false negative detection rate does not change. Based on these simulation results, we can get the following result. As r increases and s decreases, the dependability in the group management increases. r and s are not independent though. They are fixed variables according to choose particular detection mechanism and generally if r increases, s also increases and if r decreases, s also decreases.

We can think various detection mechanisms which are applicable to the intrusion tolerant system and each detection mechanism has its own r and s. If some detection mechanisms have good performances, perhaps

their r variables are relatively low and s variables are relatively high. However the dependability requirements are different according to the particular system. For example, in case of p=0.1, the most adequate r of the detection mechanism is 0.6. In case of p=0.2, r=0.7. In case of p=0.3, r=0.8. Therefore we can choose the detection mechanism which is very efficient considering the dependability and performance in the particular system.

5. Dependability Matrix for Intrusion Tolerant System

In this paper, we are analyzing the dependability according to n, m, p, r, s which are essential factors in the group management for intrusion tolerance. We mentioned that we can choose the policy that is making use of the most adequate mechanism for the particular system. Using our experiment result, we generate the following matrix.

Table 9. Dependability Matrix

n	m	p	r	s	False Positive Detection rate	False Negative Detection rate
			.....			
10			.....			
11			.....			
12	3	0.1	0.9	0.1	15.03%	0.00%
	4	0.1	0.7	0.1	15.95%	0.00%
			0.8	0.1	5.80%	0.00%
			0.9	0.1	6.53%	0.00%
				0.2	26.92%	0.00%
				0.3	52.45%	0.00%
				0.4	73.11%	0.00%
				0.5	82.74%	0.00%
		0.2	0.7	0.1	3.43%	0.00%
			0.8	0.1	3.45%	0.00%
			0.9	0.1	3.70%	0.00%
				0.2	17.56%	0.00%
				0.3	37.68%	0.00%
				0.4	56.83%	0.00%
				0.5	68.20%	0.00%
	5	0.2	0.9	0.1	0.62%	0.00%
	6	0.2	0.9	0.1	0.06%	0.19%
			.....			

From our system, we can investigate the corrupt rate p, and also extract r, s respectively for each detection mechanism. Through this matrix we can choose the most adequate m and the best detection mechanism.

6. Conclusion

The contributions of this work are as follows. First, we could extract the dependability in the intrusion tolerant system which is composed of replicated members. So we can have the reasonable data for intrusion tolerant technology about critical services like DNS and DHCP services, and anticipate its effects using that matrix. Second, we show a good reference for setting up the adequate policy using the relation between the cost and dependability that we introduce in previous analysis. Third, we suggest the method to analyze the dependability about the systems which consist of the untrusting nodes.

As a future work, we are considering the analysis of relation between the dependability and the service response time. Through the future work, we can analyze the cost and its effectiveness completely for the essential service before we deploy the intrusion tolerant technology in our service providing network.

7. Reference

1. Adelsbach, A., et. Al, "Conceptual Model and Architecture of MAFTIA," Project MAFTIA IST-1999-11583 deliverable D21.
2. Powell, D., et.al "MAFTIA (Malicious and Accidental-Fault Tolerance for Internet Applications)," Sup. Of the 2001 International Conference on Dependable Systems and Networks(DSN2001).
3. Just, J.E, and Reynolds, J.C., "HACQIT(Hierarchical Adaptive Control of QoS for Intrusion Tolerance)". In 17th Annual Computer Security Applications Conference,2001.
4. Cukier, M., et. al, "Intrusion Tolerance Approches in ITUA", In Supplement of the 201 International Conference on Dependable Systems and Networks.
5. M. Castro, B. Liskov, "Practical Byzantine Fault Toler-

ance", Proc. Of the 3rd Symposium on Operating System Design and Implementation Feb. 1999.
6. Intrusion Tolerance by Unpredictable Adaptation(ITUA), BBN, Illinois Univ, Boeing
7. ITDOS : Intrusion-Tolerant Distributed Object Systems, NAI.
8. SITAR : A Scalable Intrusion-Tolerant Architecture for Distributed Services Survivability Validation Framework, MCNC, Duke Univ.
9. James Patrick Lyons, "A Replication Protocol for An Intrusion-Tolerant System Design", University of Pennsylvania, 2000.
10. Harigovind Venkatraj Ramasamy B.engr, "A Group Membership Protocol for An Intrusion-Tolerant Group Communication System", Anna University, 1999.
11. Adnan Agbaria, Roy Friedman, "Overcomming Byzantine Failures Using Checkpointing".
12. G. Bracha and S. Toueg, "Asynchronous Consensus and Broadcast Protocols", Journal of the ACM.
13. Prashant Pandey, B.ENGR, "Reliable Delivery and Ordering Mechanisms for an Intrusion-Tolerant Group Communication System", Birla Institute of Technology and Science, 1999.
14. Michael K. Reiter, "Reliable and Atomic Group Multicast in Rampart", AT&T Bell Laboratories, Holmdel, New Jersey, U.S.A.
15. Harigovind V, Ramasamy, Michel Cukier, "Formal Verification of an Intrusion-Tolerant Group Membership Protocol", IEICE TRANS, December 2003, No 12, Vol. E86-D.

김 형 종 (hkim@swu.ac.kr)

1996년 성균관대 정보공학과 공학사
1998년 성균관대 정보공학과 공학석사
2001년 성균관대 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년 한국정보보호진흥원 수석연구원
2004년~2006년 미국 카네기멜론대학 CyLab Visiting Scholar
2007년~현재 서울여자대학교 컴퓨터학부 전임강사

관심분야 : 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 침입감내기술

이 태 진 (tjlee@kisa.or.kr)

2003년 포항공과대학교 컴퓨터공학과 공학사
2004년~현재 연세대학교 컴퓨터공학 석사과정
2003년~현재 한국정보보호진흥원 주임연구원

관심분야 : 무선 네트워크 및 VoIP 보안, 침입감내기술