동등형망여벌복사체계의 성능개선에 대한 연구

김원철, 조국

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《첨단돌파전은 현대과학기술의 명맥을 확고히 틀어쥐고 과학기술의 모든 분야에서 세계를 앞서나가기 위한 사상전, 두뇌전입니다.》(《조선로동당 제7차대회에서 한 중앙위원회 사업총화보고》 단행본 39페지)

우리는 동등형(P2P)망기술과 암호화화일[1]을 리용하여 여벌복사봉사기의 성능병목현상과 체계구축비용을 줄이였다.

암호화화일을 리용한 여벌복사체계는 요청동등마디들에서 실현되므로 여벌복사체계의 성능을 개선할수 있다.

우리는 중심화된 P2P기술[2]과 암호화화일[1]을 리용하고 여벌복사처리와 보안기능을 요청동등마디들로 분산시켜 P2P여벌복사체계의 성능을 개선하였다.

1. 암호화화일을 리용한 동등형망여벌복사체계

콤퓨터망을 리용한 여벌복사체계[3, 4]는 자료대피를 위한 전용봉사기리용으로 하여 체계구축비용이 높으며 비용을 줄이는 P2P여벌복사체계들도 분산하쉬표 DHT를 리용하는것으로 하여 여벌복사성능이 낮다.

중심화된 P2P구성방식으로 실현한 P2P여벌복사체계의 구조는 그림과 같다.

중심화된 P2P화일공유체계에서의 색인봉사기는 여벌복사관리봉사기로서 여벌복사자료를 보관하는 동등마디들의 공개열쇠증명서와 여벌복사동등마디들의 정보, 여벌복사자료들의 상태정보를 유지관리한다.

중심화된 P2P화일공유체계에서 화일봉사기능을 담당하는 동등마디는 여벌복사동등마디로서 여벌복사되는 자료들의 보관과 자료무결성을 담보한다. 여벌복사동등마디는 여벌복사관리봉사기에 가입하여 여벌복사동등마디로 등록한 다음 공개열쇠증명서와 자기의 성능정보들을 여벌복사관리봉사기에 등록하고 요청동등마디의 여벌복사요청들과 회복요청들을 처리한다.

중심화된 P2P화일공유체계에서 요청동등마디는 화일의 여벌복사를 요청하고 여벌복사화일의 기밀성과 무결성을 보장한다.

요청동등마디는 여벌복사동등마디들에 자기의 국부화일들을 여벌복사하거나 여벌복사한 화일들을 내리적재한다.

요청동등마디의 여벌복사의뢰기는 사용자의 요구나 규정된 시간에 지정된 등록부의 화일들을 여벌복사하거나 회복을 진행한다. 이때 여벌복사의뢰기는 요청동등마디의 IP주소와 여벌복사요청시점의 날자, 시간, 분정보에 기초하여 여벌복사자료의 식별자를 구성한다.

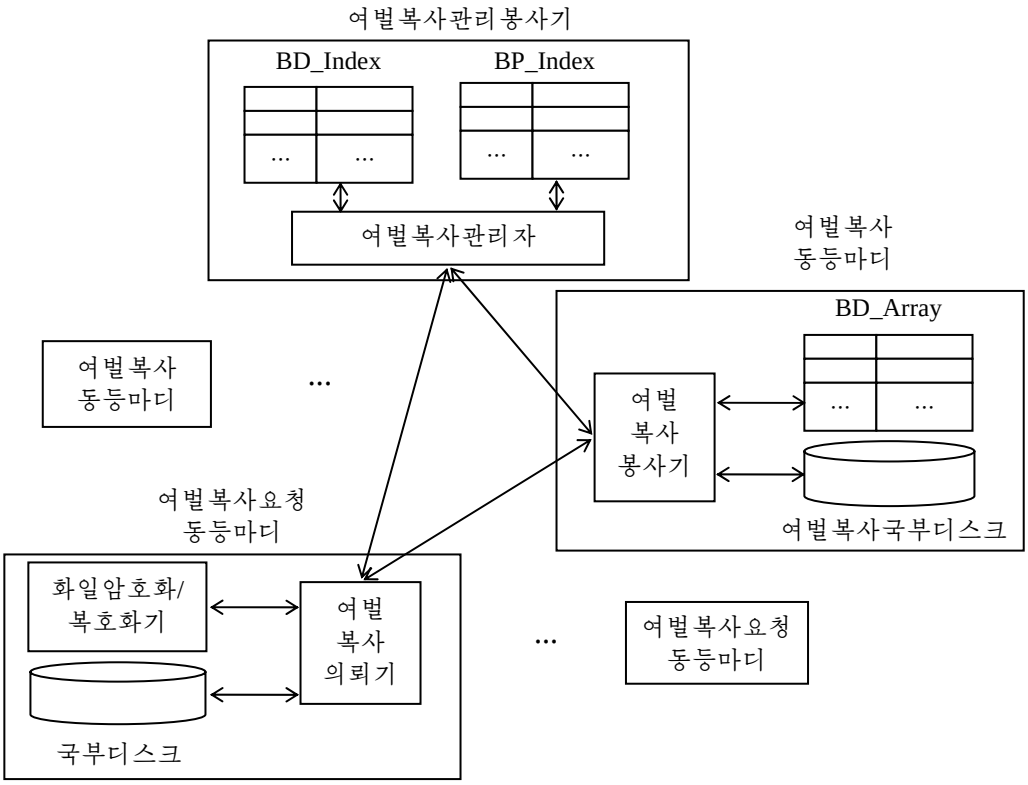

그림. P2P여벌복사체계의 구조

요청동등마디의 여벌복사의뢰기에서 여벌복사과정에 진행되는 암호화화일창조와 올리적재처리과정은 다음과 같다.

process_C_backup(file)
read(file)
K ← Gen()
d-file = Enc_K(file)
CK = $PEnc_{Ku\_c}$(K)
S_c = $PEnc_{Kp\_c}$(H(d-file ‖ CK))
m-file = CK ‖ S_c
cb-file = d-file ‖ m-file
S = create_struct_FILE_ID
S－>day = day
S－>time = time
S－>minute = minute
S－>IP_c = IP_c
BD_ID = S
upload(cb-file, BD_ID)
End

요청동등마디의 여벌복사의뢰기는 화일암호화기를 호출하여 여벌복사되는 화일을 암호화한다. 화일은 여벌복사되기 전에 암호화되며 리용된 암호화열쇠는 소유자의 공개열쇠로 암호화된다.

요청동등마디의 여벌복사의뢰기에서 회복처리과정에 진행되는 여벌복사자료의 탐색과 내리적재, 화일복호화과정은 다음과 같다.

process_C_recovery(IP_{ci}, day_i, $time_i$, $minute_i$)
    A_search(BD_Index, IP_{ci}, day_i, $time_i$, $minute_i$)
    B_upload(B_ID)
    d-file, CK, S_c, ← Extract(cb-file)
    if $PDec_{Ku\_c}(S_c) = H(\text{d-file} \parallel CK)$
        $K = PDec_{Kp\_c}(CK)$
        $file = Dec_K(\text{d-file})$
    save(file)
End

2. 동등형망여벌복사체계의 성능평가

론문에서 제안한 암호화화일을 리용한 P2P여벌복사체계(CF_backup)를 Securebackup[3]과 같은 크기의 화일자료들에 대한 여벌복사와 회복시의 계산지연으로 평가하였다.(표)

결과는 붉은별 2.0, 처리기주파수 2.4GHz, 주기억 2GB인 콤퓨터에서 대칭열쇠암호화로 AES(256bits), RSA(2048bits)알고리듬을 리용한 측정결과이다.

표. 암호화화일을 리용한 P2P여벌복사체계의 성능

구분 / 크기/KB	여벌복사(올리적재)				회복(내리적재)			
	Securebackup		CF_backup		Securebackup		CF_backup	
	평문/ms	암호화/ms	평문/ms	암호화/ms	평문/ms	암호화/ms	평문/ms	암호화/ms
500	4 000	5 000	79	165	4 300	6 000	94	191
1 000	11 000	13 500	172	281	8 000	14 000	172	313
1 500	15 000	16 000	219	375	10 500	17 000	250	437
2 200	17 500	21 000	329	584	16 500	20 500	344	532
2 600	19 000	25 000	390	672	19 500	26 000	406	609
3 000	24 000	26 500	453	749	22 500	29 500	469	703

우의 성능평가에서 알수 있는바와 같이 암호화화일을 리용한 P2P여벌복사체계는 Securebackup에서의 위상구조유지와 관리를 위한 처리비용이 없으며 색인봉사기의 탐색에 의하여 여벌복사동등마디가 직접 결정되므로 여벌복사체계의 성능을 크게 개선한다. 또한 암호화화일을 리용한 P2P여벌복사체계에서 보안기능들은 요청동등마디들에서 진행되므로 대용량자료의 여벌복사처리와 회복처리에서 여벌복사동등마디들의 병목현상을 발생시키지 않으므로 전반적인 체계성능을 개선한다.

맺 는 말

P2P기술과 암호화화일을 리용하여 여벌복사체계를 실현하고 성능을 평가하였다. 제안한 P2P여벌복사체계는 체계구축비용을 줄이고 여벌복사처리과정의 보안처리를 동등마디들로 분산시킴으로써 여벌복사봉사기들의 병목현상을 줄이고 성능을 크게 개선할 수 있다.

참 고 문 헌

[1] Kim Won Chol; 21st International Conference on Advanced Information Networking and Applications Workshops, 1, 432, 2007.

[2] R. Steinmetz, K. Wehrle; Peer-to-Peer Systems and Applications, Springer, 55~72, 2005.

[3] Houssem Jarraya, Maryline Laurent; Computer & Security, 29, 180, 2010.

[4] Abdulhalim Dandoush et al.; Computer Networks, 64, 243, 2014.

주체108(2019)년 2월 5일 원고접수

Research on the Performance Improvement in the P2P Backup System

Kim Won Chol, Jo Kuk

In this paper, we have improved the performance in the P2P backup system by using the centralized P2P architecture and the encrypted file with the key management function.

Key words: P2P, backup