제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

# 액티브 네트워크에서의 도메인 기반 키관리 스킴에 관한 연구

신종회*, 박희운**, 한상범*, 서혜숙*, 김태윤*
*고려대학교 컴퓨터학과
**한국정보보호진흥원 기술표준팀
e-mail: jshin9@netlab.korea.ac.kr

# A Study on Domain-based Key Management Scheme for Active Network

Jong-Whoi Shin*, Hee-Un Park**, Sang-Beom Han*,
Heyi-Sook Suh*, Tai-Yun Kim*
*Dept of Computer Science & Engineering, Korea University
**Korea Information Security Agency

요 약

액티브 네트워크는 현존하는 공유기반의 네트워크에 대하여 새로운 기술과 서비스, 표준 등을 적용하기가 어렵고 또한, 여러 프로토콜 계층에서 중복된 운영이 발생한다는 문제점을 해결하기 위해 등장하였다. 액티브 네트워크는 패킷에 실행 가능한 코드를 탑재하여 전송할 수 있으며, 이러한 코드의 실행은 네트워크 노드에 대한 상태변경이 가능하다. 그러나, 네트워크 노드가 공유기반 네트워크에 위치한 상황에서는 보안과 안전성 문제가 해결되어야 하며, 이를 위해 기존의 인증, 권한부여, 비밀성, 무결성 등과 같은 보안사항이 요구된다. 여기에는 보안의 핵심적인 요소인 암호키가 관련하게 됨에 따라 본 연구에서는 광범위한 액티브 네트워크의 보안성 확보를 위해 사용되는 암호키를 도메인에 기반하여 관리하는 스킴을 제안하고자 한다.

## 1. 서론

액티브 네트워크의 개념은 현존하는 공유기반의 네트워크에 대하여 새로운 기술과 서비스, 표준 등을 적용하기가 어렵고 또한, 여러 프로토콜 계층에서 중복된 운영이 발생한다는 문제점을 해결하기 위해 등장하였다[1]. 즉, 전통적인 데이터 네트워크는 단순하게 하나의 종단시스템으로부터 다른 시스템으로 비트를 전송하는 기능만을 수행했다. 이와 같은 네트워크 상에서의 연산기능은 패킷 스위치 네트워크에서의 헤더처리, 연결지향 네트워크에서의 신호처리와 같이 극도로 제한적인 부분에 한해서 수행된다. 액티브 네트워크는 사용자 데이터에 대한 커스터마이즈된 연산을 수행함으로써 이와 같은 전통적인 개념을 전환시키게 되었다. 예를 들면, 액티브 네트워크에서의 사용자는 네트워크의 노드에게 커스터마이즈된 압축 프로그램을 전송할 수 있으며 또한, 수신단에서 패킷 처리 시 프로그램을 실행하도록 노드에 요구할 수 있다[2]. 다시 말해, 액티브 네트워크는 네트워크 응용에 맞도록 통신 프로세스를 커스터마이즈할 수 있는 소프트웨어적인 프레임워크를 제공하는 것이다. 액티브 네트워크는 캡슐이라 불리는 패킷에 실행 가능한 코드를 탑재하여 전송하게 되는데, 이러한 코드의 실행에 따라 네트워크 노드에 대한 상태변경이 가능하다는 장점이 있다. 하지만 이러한 장점은 네트워크 노드가 공유기반 네트워크에 위치하기 때문에 보안과 안전성이 반드시 보장되어야 한다는 문제를 유발하게 되었다. 액티브 네트워크의 보안과 안전성 확보를 위해서는 기존의 인증, 권한부여, 비밀성, 무결성 등과 같은 보안요구사항이 확보되어야 하며, 여기에는 보안의 핵심적 요소인 암호키가 관련하게 된다. 이에, 본 연구에서는 광범위한 액티브 네트워크의 보안성 확보를 위해 사용될 것으로 예상되는 암호키를 도메인에 기반하여 관리하는 스킴을 제안하고자 한다.

## 2. 액티브 네트워크에서의 보안위협

액티브 네트워크는 기존의 네트워크에 비해 위협과 공격에 쉽게 노출될 수 있다. 네트워크 노드에 대한 상태를 변경하는 실행코드가 캡슐에 담겨져 전송되기 때문에 수신 노드에서는 인가된 송신자에 의한 패킷인 지 여부를 인증해야할 뿐만 아니라 실행코드에 대한 정확한 연산이 수행되어야 한다.

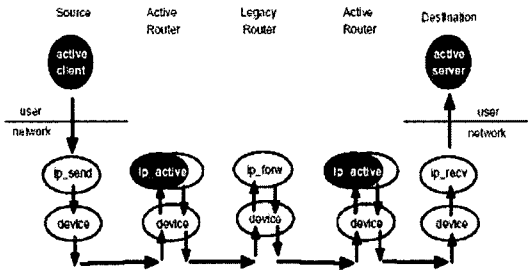


그림1. 액티브 네트워크에서의 응용처리

그림1과 같은 액티브 네트워크에서의 응용처리시, 발생 가능한 보안위협에는 정보변조, 정보유출, 서비스 훔치기, 서비스 거부, 복합공격 등의 위협이 있다[3][5].

- 정보변조 : 권한이 없는 상태에서 악의적으로 데이터를 변경하는 행위
- 정보유출 : 정보에 대한 서비스 권한이 없는 사람에게 정보를 유출하는 행위
- 서비스 훔치기 : 권한이 없는 사용자가 마치 권한이 있는 사람처럼 서비스를 사용하는 행위
- 서비스 거부 : 의도적으로 네트워크 자원 및 서비스를 방해하거나 완전히 막아버리는 행위
- 복합공격 : 액티브 노드에 가장 큰 위협으로 악의적인 사용자가 대량의 액티브 패킷을 중앙 라우터에 전송하여 모든 대역폭을 소비함으로써 시스템을 다운시키는 행위

특히, 서비스 거부 공격은 다루기 어려운 문제로 유형을 살펴보면 다음과 같다.

- 제한자원의 소모 : 네트워크의 연결(TCP-SYN flooding), 포화 대역폭(UDP floods, 위조된 ICMP Echo 메시지공격, 스팸 등) 그리고 다른 자원들을 고갈시키는 공격
- 구성정보의 변경 또는 파괴
- 구성요소의 물리적 파괴 및 변경

## 3. 액티브 네트워크의 보안방법

전통적인 보안의 개념에는 인증, 접근 통제, 암호화 등이 포함된다. 액티브 네트워크 응용과 라우터는 상호 인증을 통해 신뢰성에 대한 근거를 확보하게 되며, 암호화와 전자서명은 코드와 데이터를 포함하고 있는 액티브 네트워크 캡슐의 무결성과 프라이버시를 보호할 수 있게 된다[4]. 액티브 네트워크 환경에서 사용될 수 있는 보안기법에는 크게 액티브 노드에 대한 보호기법과 액티브 패킷에 대한 보호기법으로 나눠 볼 수 있다[5].

### 3.1 액티브 노드 보호기법

액티브 노드 보호를 위한 기법에는 액티브 패킷 인증, 모니터링 및 제어, 제한, 검증전달코드 등의 기법이 있다.

- 패킷 인증은 공개키 서명 알고리즘과 같은 알고리즘을 이용하여 만들어진 인증서를 갖고 신원을 보장하는 기법
- 모니터링 및 제어기법은 액티브 패킷의 사용과 접근이 허용된 정보, 시스템 자원 및 서비스를 제한하기 위해 참조모니터를 사용하는 기법
- 제한기법은 액티브 패킷의 실행시간, 패킷이 전달되는 노드의 범위 제한, 패킷의 중복횟수 제한과 같은 제한을 두어 액티브 패킷이 노드의 자원을 독점하는 것을 막는 기법
- 검증전달코드(PCC: Proof Carrying Code) 기법은 정확성에 대한 증명서를 각 액티브 패킷 내에 이동프로그램과 한 쌍으로 전송하는 기법

### 3.2 액티브 패킷 보호기법

액티브 패킷 보호를 위한 기법에는 암호화 기법, 결함감내기법 등이 있다.

- 액티브 패킷의 특성으로 인해 각 중간노드에서도 패킷에 대한 암호화나 복호화가 가능해야하고 패킷경로 또한 동적으로 변경된다. 따라서, 액티브 패킷을 통해 전송된 프로그램이 암호화되었다고 할지라도 노드에서 수행하려면 복호화되어야 하기 때문에 이동암호화의 개념이 필요하다[6].
- 결함감내기법에는 복사, 보존, 방향재설정이 있

다. 복사는 패킷을 각 노드에 복사하는 것이며, 보존은 노드 결함에 대비하여 패킷을 일시적으로 저장하는 것이다. 방향재설정은 설정된 기본 경로가 두절되었을 경우 대체 경로를 찾아내는 것이다. 복사와 보존 방법은 메모리와 대역폭을 많이 차지하여 네트워크 패킷에 적합하지 않은 방법이다. 방향재설정과 암호화기법은 기본적으로 CPU 싸이클만을 소비하기 때문에 패킷보호에 대해 보다 넓은 응용을 갖을 수 있다.

## 4. 도메인 기반의 키관리 스킴

### 4.1 도메인 기반의 개념

기존 네트워크에서의 암호화 기법은 전체 네트워크 경로를 모두 보호해야 할 지라도 두 종단간 즉, 송신지와 목적지간에서만 암호화 과정이 수행된다. 그러나, 액티브 네트워크에서는 액티브 패킷이 보통 프로그램 코드와 데이터가 전송되므로 기존의 암호화 기법은 종단간에서만 암호화하는 반면, 액티브 패킷의 특성으로 인해 내용을 액세스할 필요가 있는 중간 노드들에 대해서도 암호화를 수행 해야한다[7]. 본 연구에서는 이와 같은 특성을 반영하여 액티브 네트워크를 구성하고 있는 액티브 노드(예: 라우터 또는 스위치)들 중 특정 프로그램이 실행되어야하는 대상 노드 그룹을 하나의 도메인으로 설정하고, 이러한 도메인 구성원간 인증, 접근제어, 무결성, 부인봉쇄, 비밀성 등을 보장하는 키관리 메커니즘을 제안하고자 한다. 도메인 기반의 키관리 메커니즘은 도메인 구성에 있어 최소한의 키갱신이 가능하며, 구성원에 대한 동적인 관리를 수행할 수 있다. 또한, 도메인 구조를 제어부와 패킷 전송부로 구분하여 키관리자의 오버헤드를 줄이고, 액티브 패킷 전송 시 발생할 수 있는 각종 위협을 방지할 수 있게 된다. 도메인 기반의 키관리 스킴은 기본적으로 구성원 인증 및 패킷 암호화를 위해 공개키기반 구조를 적용함을 원칙으로 한다. 공개키기반구조의 적용은 액티브 네트워크 상에서 키관리의 효율성 및 이식성을 높일 수 있는 특성을 지니고 있어 도메인 기반 구조와 더불어 보다 효율적인 키관리가 가능할 것으로 기대된다.

### 4.2 키관리 스킴 제안

#### 4.2.1 구성 요소 및 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성 요소를 나타낸 것이다.

- $DKM_i$ : 도메인 키 관리자 i
- $DKA_i$ : 도메인 키 중간 관리자 i
- $DME_{list}$ : 도메인 구성원 목록
- $SDB_i$ : 서브 도메인 Border i
- N, $DMB_i$ : 노드(라우터) 및 도메인 Border i
- $ADB_i$ : 액티브 도메인 Border i
- PKM : 각 관리자들 및 Border의 공개키 관리자
- $DME_i$, DI : 도메인 구성원 i 및 도메인 초기설정자
- AKey : PKM에 의해 생성된 액티브 키
- $K_{P\_DKM_i}$, $K_{P\_DKA_i}$ : $DKM_i$의 공개키 및 $DKA_i$의 공개키
- $K_{P\_B_i}$ : 각 $B_i$의 공개키
- $K_{DKM_i\_DKA_i}$ : $DKM_i$와 $DKA_i$ 사이의 공통키
- $K_{DME_i}$ : 도메인 구성원 $DME_i$의 비밀키
- $K_{DKA_i\_DME_s}$ : 각 $DKA_i$가 관리하는 구성원들과의 공통키
- Hdr : 각 도메인의 식별 정보
- $ID_*$, $Sig_*$, $IP_*$ : *의 식별자, 서명 및 IP 주소
- M : 패킷

#### 4.2.2 시스템 프로토콜

**1) 도메인 초기화 단계**

①$DKM_i$, $DKA_i$ 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 $PKM_i$으로부터 수신한다.

②각 도메인은 $DKM_i$를 정점으로 구성원들을 분할하여 담당하는 각 $DKA_i$를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

**2) 도메인 구성 단계**

①도메인 초기설정자(DI)는 도메인 구성원 목록($DME_{list}$)을 작성하여 자신의 식별자 $ID_{DI}$를 연접하여 서명을 수행한 다음 $PKM_i$에게 전송한다.

$Sig_{DI}(ID_{DI}||DME_{list}) \rightarrow PKM_i$, $DME_{list} = (ID_{DME1}||\cdots||ID_{DMEn})$

②$PKM_i$은 서명 확인을 통해 DI 및 $DME_{list}$를 인증하고 액티브 패킷 서비스를 위한 AKey를 생성한다. 단, AKey는 도메인이 형성될 때, 오직 관련된 Border들에게만 제공함으로서 신뢰성을 높이고 있다.

③PKM은 해당 Domain에 공개키를 이용하여 안전하게 $DME_{list}$를 전송한다.

**3) 도메인 구성원 가입 단계**

①$DKM_i$는 도메인 내에서 $DKA_i$와의 비밀통신 시 사용할 $K_{DKM_i_DKA_i}$를 생성하여 유니캐스트 채널을 통하여 안전하게 $DKA_i$에게 전송한다.

②도메인에 구성원으로 가입될 각 노드들은 자신의 서명을 이용하여 $DKA_i$에게 자신을 인증하고 자신의 비밀키 $K_{DME_i}$를 $K_{P_DKA_i}$로 암호화하여 안전하게 전송한다.

③$DKA_i$는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 도메인 구성원 목록을 생성해 $DKM_i$에게 전송한다.

④$DKM_i$는 각 $DKA_i$로부터 수신된 도메인 구성원 목록에 대해 복호 및 인증을 수행한 다음 $DME_{list}$와 비교 확인한다.

⑤$DKA_i$는 수신된 비밀키 $K_{DME_i}$를 이용하여 각 구성원에게 $K_{DKAi_DMEs}$를 안전하게 전송해 준다. 동시에, 이 $K_{DKAi_DMEs}$는 $DKM_i$ 및 $SDB_i$에게 안전하게 전송된다.

**4) 액티브 패킷 전송 단계**

①각 구성원들은 $K_{DKAi_DMEs}$를 이용하여 액티브 패킷 M을 암호화한 다음 Border $SDB_i$에게 전송한다. $K_{DKAi\_DMEs}(M) \rightarrow SDB_i$

②$SDB_i$는 암호화되어 수신된 정보를 복호화하여 Hdr를 확인하고 Hdr이 없다면 액티브 패킷 M을 AKey로 암호화하여 각 $SDB_i'$에게 전송한다.

③각 $SDB_i'$는 수신된 정보를 복호화하고 이를 자신이 속한 도메인의 공통키로 암호화하여 도메인 구성원들에게 전송한다.

④각 서브 도메인의 구성원 $DME_i'$는 $K_{DKAi_DMEs}'$로 수신된 정보를 복호화하여 메시지를 확인한다. 기타 메시지 전송은 상기 프로토콜에 기초해 수행된다.

**5) 신규 구성원 가입 및 기존 구성원 탈퇴 단계**

①신규 구성원 가입은 3) 도메인 구성원 가입 단계와 같은 과정을 수행한다.

②기존 구성원 탈퇴 시에는 $DKA_i$가 새로운 $K_{DKAi_DMEs}'$를 생성하여 남아 있는 구성원들 $DME_i'$, $DKM_i$ 및 $SDB_i$에게 안전하게 전송함으로서 키 갱신을 수행한다.

## 5. 결론 및 향후과제

본 연구는 액티브 네트워크의 보안과 안전성 확보를 위해 제공되는 인증, 비밀성, 무결성과 같은 기능에 대하여, 그 핵심요소인 암호키를 도메인에 기반하여 관리할 수 있는 스킴을 제안한 것이다. 이러한 키관리 스킴은 방대한 액티브 네트워크에서 도메인에 기반하여 키관리를 수행함으로써 기존의 키관리 메커니즘보다 효율적으로 키를 관리할 수 있을 것으로 예상된다.

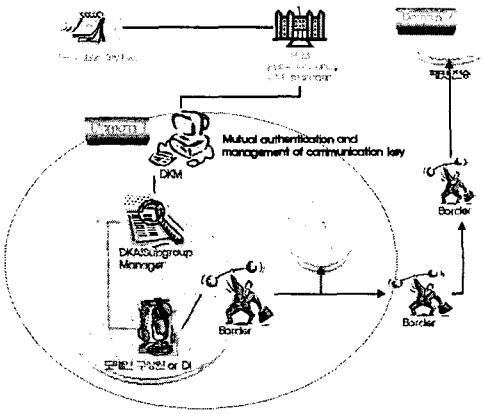


그림2. 제안된 키관리 스킴 구조도

향후에는, 키관리 설정 후 일정시간이 경과된 뒤 설정키를 재설정하는 메커니즘 개발, 효율적 키공유 메커니즘 개발, 테스트 베드를 이용한 도메인 기반 키관리의 성능 테스트 연구 등이 필요할 것으로 예상된다.

## 참 고 문 헌

[1] David L.Tennehouse, *et al.*, "A Survey of Active Network Research", IEEE Com. 1997

[2] David L. Tennenhouse and David J. Wetherall, "Towards an Active Network Architecture", Comp. Commun. Rev. vol 26, no 2, Apr. 1996

[3] "Security Architecture for Active Nets", AN Security Working Group, Jul. 1998, Modified by Seraphim Group, May 2000

[4] Roy H. Campbell, *et al.*, "Seraphim: Dynamic Interoperable Security Architecture for Active Networks", IEEE OPENARCH 2000

[5] K. Psounis, "Active Networks: Applications, Security, Safety, and Architectures", IEEE Communication Surveys, 1999

[6] J.M. Park, K.J. Chae, "Active Network Security Technology Trend", Sigcomm Review, Dec. 2000

[7] Y.S. Kim, J.C. Na, S.W. Sohn, "A Secure Method for Transferring Active Packets", Proc. of WSEAS'01, Cairns, Australia, Dec.17~21. 2001