유비쿼터스 환경에서의 믹스-넷 적용을 위한 다양한 암호화 알고리즘 및 키 길이 사용 방안*

김인환°, 김종욱, 홍만표
아주대학교 정보통신전문대학원
{tlrks°, kju, mphong}@ajou.ac.kr

The method of using various encryption algorithms and key sizes for applying a mix-net to the ubiquitous environment

Inhwan Kim°, JongUk Kim, ManPyo Hong
Graduate School Information and Communication, Ajou University

1. 서 론

IT 분야의 관심 대상 중 하나인 유비쿼터스(Ubiquitous)는 사용자에게 특정한 서비스 제공을 위해 분산되어 있는 센서로부터 개인 정보를 수집하는 일이 빈번하게 발생한다. 정보의 이동이 빈번하다는 것은 그만큼 정보의 유출이 많이 발생할 수 있다는 것을 의미하므로 개인 정보의 보호를 위한 시스템의 구성은 중요한 이슈라 할 수 있다.

2. 관련 연구

개인 정보 보호를 위한 연구 중 하나인 믹스(mix)는 1981년 David Chaum에 의해 제안된 후, *메시지의 내용*뿐만 아니라 *누가 누구와 통신하는지*에 대한 정보까지도 보호할 수 있는 방법으로 꾸준히 연구되어왔다. 기존의 믹스 시스템들은 대부분 사용자의 익명성 강화에 중점을 두어 속도 측면에서 사용자에게 만족할만한 성능을 보여주지 못했다. 또한, 고정된 암호화 알고리즘을 사용함으로써 성능이 낮은 노드에 적용하는데 한계가 있다.

3. 본 론

암호화 알고리즘은 컴퓨팅 파워에 따라 소요 시간이 다르다. 예를 들어 PDA처럼 낮은 처리 속도의 중앙처리장치를 사용하는 노드와 데스크탑과 같이 빠른 처리 속도의 중앙처리장치를 사용하는 노드는 암호화 과정에 필요로 하는 시간이 다르다. 특히 믹스에서는 겹암호화(onion encryption)를 수행하므로 암호화에 필요한 시간은 더욱 차이가 난다. 또한 저전력을 이용하는 센서와 같은 노드는 암호화에 필요로 되는 많은 컴퓨팅 파워로 인해 배터리 문제가 생기게 된다.

저성능/저전력 기기가 믹스에 참여하는 상황에서의 믹스-넷 적용을 위해서는 네트워크를 구성하는 기기의 성능을 고려하여 암호화 알고리즘 및 키 길이를 사용하는 것이 중요하다. 예를 들어 저성능 기기는 대칭 키 암호화로 DES 56-bits 키를 사용하고, 비대칭 키 암호화로 RSA 512-bit를 사용하며, 고성능 기기는 대칭 키 암호화로 AES 256-bits를 사용하고, 비대칭 키 암호화로 RSA 2048-bit를 사용할 수 있다. 이 방법을 이용한 믹스 시스템은 "사용자 및 믹스가 믹스-넷을

* 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스 컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임

구성하는 믹스들이 사용하는 암호화 알고리즘, 키 길이, IP 주소를 알고 있다."라는 가정에서 아래와 같이 설명될 수 있다.

표 1. 표기법 정의

K_n	n-번째 믹스의 공개 키(Public key)	K_a	수신자의 공개 키
SK_n	n-번째 믹스의 비밀 키	M	메시지
A	최종 수신자의 주소	A_n	n 번째 믹스의 주소

사용자가 믹스 패킷을 생성하기 위해서는 먼저 메시지 M을 수신자의 공개 키 K_a로 암호화한다. 그 후, SK_n과 A를 포함하는 서브 헤더(sub-header)를 만들고, 앞에서 암호화한 메시지와 연결하여 붙인다. 여기서 생성한 서브 헤더의 내용을 보호하기 위해 현재까지 만든 패킷의 시작부분부터 K_n을 이용하여 K_n의 키 길이만큼 암호화한다. 이 때, 서브 헤더에서 SK_n가 있는 부분이 K_n으로 암호화되는 부분에 포함되어야 한다. K_n에 의해 암호화된 후 남은 부분을 SK_n으로 암호화한다. 여기까지 생성한 패킷은 하나의 믹스에 해당하는 정보를 포함하는 것으로, 위의 과정을 따라 n-1번째 믹스부터 1번째 믹스까지의 정보를 이용한 서브 헤더를 역으로 생성한 후, 하나의 완성된 믹스 패킷을 만든다.

경로에 있는 믹스에서, 수신한 메시지를 처리하기 위해 사용되는 암호화 알고리즘과 키는 믹스마다 다르지만, 위에서 언급한 가정에 의하면 믹스 패킷의 서브 헤더는 해당 믹스에서 사용하는 암호화 알고리즘을 이용하여 암호화되어 있다. 따라서 각 믹스는 자신이 결정한 암호화 알고리즘 및 키를 이용하여 수신한 믹스 패킷을 처리할 수 있다. 먼저 믹스는 받은 패킷의 앞 부분에서부터 자신이 사용하는 비대칭 키 길이만큼 자신의 개인 키(Private Key)로 복호화 한다. 이 과정에서 얻은 비밀 키(혹은 비밀 키를 생성하는데 쓰일 정보)를 이용하여 나머지 부분을 복호화한다. 해당 노드에 대한 암호화 부분이 모두 복호화된 후 패킷 헤더에서 다음 노드에 대한 정보를 얻은 후 그 정보를 이용하여 메시지를 전송한다.

보안 분야에서 우려하는 문제 중 하나는 아무리 잘 구성된 보안 시스템일지라도 보안이 약한 부분이 한군데라도 있다면 그 시스템은 안전하지 못하다는 것이다. 사방에 견고한 벽을 쌓아두더라도 한 곳이 뚫린다면 그 벽들이 쓸모 없게 되는 것과 마찬가지이다.

메시지 기밀성(confidentiality)과 사용자의 익명성을 보장하기 위한 믹스 시스템에서 필수 구성요소인 암호화에 사용되는 알고리즘과 키 길이를 다르게 한다는 것은 앞서 언급한 보안 문제를 야기시킬 수 있는 것처럼 보인다. 즉, 공격자가 저성능 기기의 약한 암호화 알고리즘을 깨뜨린다면 본 논문에서 제안한 방법이 익명성을 제대로 보장하지 못하는 것이 아닐까 하는 우려를 할 수 있다. 그러나 PDA와 같은 저성능 기기의 믹스가 제공하는 암호화 과정이 안전하지 못할지라도, 그 앞뒤에 존재하는 상대적으로 안전한 암호화를 사용하는 믹스에서 익명성을 보장하기 때문에 믹스-넷은 제 기능을 수행할 수 있다.

4. 결 론

믹스 시스템은 익명 통신을 위해 많은 암호화 과정을 필요로 한다. 이는 믹스로 사용되는 노드의 부담이 크다는 것을 의미한다. 본 논문에서는 휴대폰, PDA와 같은 저성능 기기가 통신의 주체가 되는 일이 잦은 유비쿼터스 환경에 믹스를 적용하기 위해, 노드의 성능에 맞는 암호화 알고리즘과 키 길이를 사용하는 방안을 제시하였다. 이 방법은 믹스의 겹암호화 과정에서 발생하는 부하를 감소시킴으로써 PDA, 센서와 같은 저성능 기기가 많이 사용되는 유비쿼터스 환경에 더 합리적이다.