*믹스 네트워크에서 저성능 송신 디바이스를 위한 부하분산 기법

이창호, 정유석, 홍만표
아주대학교 정보통신전문대학원
e-mail:{sunnyday78, j8508, mphong}@ajou.ac.kr

Load Balancing Mechanism for Low Efficient Device on Mix Network

Chang-Ho Lee, Yoo-Suk Jung, Man-Pyo Hong
Dept of Information and Communication, Ajou University

요 약

익명통신이란 통신주체인 송수신자에게 익명성을 제공하여 누가 누구와 메시지를 주고받는지 제 삼자가 모르게 하는 것으로, 사용자 정보와 사용자 상황정보가 수집되거나 저장되는 특성 때문에 개인정보의 유출이나 남용과 같은 개인정보 침해사고의 가능성이 높은 유비쿼터스 환경에서 개인정보 보호에 대한 해결방법으로 활용될 수 있다. 본 논문에서는 대표적인 익명통신 방법이면서, 송신자가 전송할 메시지를 여러 번 암호화하기 때문에 송신자의 부하가 많은 믹스형 익명통신을 대상으로 송신자의 과도한 부하문제를 해결하면서 안전하게 익명성을 제공하기 위해 부하분산 방법을 제안하고, 제안하는 방법이 적용된 믹스 시스템에서 이루어지는 메시지 전송 프로토콜을 정의한다. 제안하는 방법을 통해서 저성능의 송신 디바이스를 사용하는 사용자들은 암호화 하는데 많은 시간이 소요되어 서비스를 제공받는데 지체되거나 서비스를 제공하지 못하는 어려움을 해결할 수 있다.

1. 서론

1980년대 말 미국 제록스사의 와이어(Weiser)에 의해 차세대 정보통신 분야의 새로운 비전으로서 유비쿼터스 컴퓨팅에 대한 개념이 제시된 이후 이에 대한 많은 연구들이 진행되고 있다. 유비쿼터스 컴퓨팅 환경에서는 인간중심의 서비스를 제공하기 위해 컴퓨팅 장치들이 매순간 발생하는 사용자의 상황을 인지하고 그 결과에 따라 자동적이며 능동적으로 대응할 것으로 예상된다. 따라서 사용자에게 제공되는 서비스 역시 컴퓨팅 장치들이 먼저 사용자의 요구를 능동적으로 파악한 뒤 가능한 최선의 서비스를 사용자에게 제공하는 형태로 이루어질 것으로 예상되는데, 이는 서비스 제공자가 사용자의 요청에 따라 수동적으로 서비스를 제공하는 지금의 방식과 차별된다.

이를 실현하기 위해서는 서비스 제공자나 시스템이 사용자 정보나 사용자 상황정보와 같은 개인정보를 인지하고 있어야하며 사용자에게 더욱 적합한 서비스를 제공하기 위해 더욱 많은 개인정보가 요구될 수 있다. 그러나 이는 사용자 개인정보 유출이나 악용과 같은 개인정보 침해사고 유발의 가능성을 높이기 때문에 유비쿼터스 환경에 대한 신뢰성 문제를 야기할 수 있다.

개인정보 보호에 대한 기술적인 해결방법중 하나로 익명통신이 활용될 수 있는데, 익명통신이란 통신주체인 송수신자에게 익명성을 제공하여 누가 누구와 메시지를 주고받는지 제 삼자가 모르게 하는 것을 말한다[1]. 통신주체들의 신원정보가 노출되지 않는 특성 때문에 익명통신은 개인정보 침해사고가 심각한 문제로 야기될 수 있는 전자선거, 전자화폐, 전자우편 등의 분야에 활용될 수 있으며 이에 대한 많은 연구가 진행되어 왔다.

익명통신을 제공하는 시스템으로는 믹스넷(Mix-net), 디씨넷(DC-net), 셔플넷(Shuffle-net), 토르(Tor), 크라우드(Crowds) 등 많은 시스템들이 있는데, 본 논문에서는 전송할 메시지들을 여러 번 암호화하기 때문에 송신자의 부하가 많은 믹스형 익명통신을 대상으로 송신자의 과도한 부하(load) 문제를 해결하면서 안전하게 익명성을 제공할 수 있는 방법을 제안하고, 제안하는 방법이 적용된 믹스 시스템에서 이루어지는 메시지 전송 프로토콜을 정의한다.

2. 관련연구

이 장에서는 본 논문에서 제기하는 문제와 관련하여 기존의 믹스형 익명통신 시스템들이 어떤 문제점을 가지고 있는지를 기술한다.

2.1. 믹스넷(Mix-net)[2]

(그림 1) 믹스넷 구성요소들의 기능 및 부하 정도

익명통신에 대한 최초의 연구는 1981년 D. Chaum의 '믹스넷(Mix-net)'이다. 그림 1은 믹스넷의 구성 및 구성요소들의 기능과 상대적인 부하 정도를 표현한다. 믹스넷에서 송신자(sender)들은 믹스(이후로는 믹스 노드라 호칭한다.)들로 이루어진 믹스 네트워크를 통해 메시지를 전송하는데, 전송과정에서 적어도 하나 이상의 믹스 노드를 신뢰할 수 있다면 수신자에게 도착한 메시지는 누구로부터 왔는지 알 수 없게 되고 믹스 네트워크 전체에서 송신자의 익명성은 보장된다. 하

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

지만 송신자들은 전송경로에 포함되는 모든 믹스 노드들의 공개키로 메시지들을 여러 번 암호화 하므로 계산량이 많다는 단점이 있다. 표 1[3]은 저성능의 PDA - Zaurus SL-C3000(416 MHz CPU / 64MB RAM)와 고성능의 노트북 - IBM Thinkpad R51(1.7 GHz CPU / 1 GB RAM)으로 암호화와 암호화에 필요한 일련의 작업을 했을 때 걸리는 시간을 측정하고 비교한 결과를 보여준다. 이 결과를 통해 만약 사용자가 저성능의 송신 디바이스를 사용한다면 서비스의 종류에 따라 메시지를 암호화 하는데 많은 시간이 소요되어 해당 서비스를 제공받는데 지체되거나 아예 서비스를 제공받지 못할 수 있음을 알 수 있다.

<표 1> 암호화에 따른 성능비교

Operation (key/date)	Time Consumption on	
	SL-C3000	Thinkpad R51
RSA Key Generation (1024bit key)	122 s	2.2 s
RSA Encryption (1024bit key, 64bit data)	172 ms	10 ms
RSA Decryption (1024bit key, 128bit data)	856 ms	40 ms
RSA Signing (1024bit key, 64bit data)	833 ms	55 ms
RSA Verification (1024bit key, 128bit data)	169 ms	5 ms
ASE Encryption / Decryption (128bit key, 2048bit data)	582 ms	35 ms
SHA-1 Hash (2048bit data)	111 ms	5 ms

2.2. 익명 프레임워크(Anonymity Framework) - *firstmix*[4]

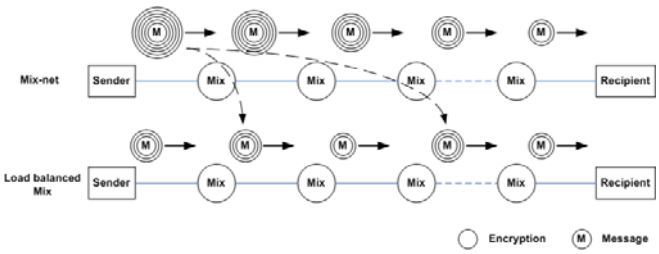
(그림 2) *firstmix* 구성요소들의 기능 및 부하 정도

2005년, 믹스넷에서 제공하는 익명통신 기술을 모바일 비즈니스(mobile business) 환경에 적용하려는 연구가 있었다. 이 연구에서는 모바일 디바이스를 사용하는 사용자들의 특성과 모바일 디바이스에 제공되는 응용프로그램들의 특성에 따라 다른 수준(level)의 익명성이 필요하다는 것을 인식했다. 따라서 익명성 수준에 영향을 끼치는 몇 개의 파라미터(parameter)들을 정의하고 이를 바탕으로 시스템을 구성하여 동적 익명성(dynamic anonymity)을 제공하는 익명 프레임워크를 제안했다. 사용자는 몇 개의 파라미터 중에서 '*path picker*' 값을 '*firstmix*'로 설정하여 메시지 전송경로 설정과 모든 암호화 작업을 첫 번째 믹스 노드가 담당하게 함으로서 송신자가 처리해야할 작업량을 줄일 수 있었고 믹스넷의 문제점인 송신자의 과도한 부하문제를 해결 할 수 있었다. 하지만 첫 번째 믹스 노드가 송수신자 모두를 알게 되기 때문에 공격자에 의해 장악된다면 익명성을 보장할 수 없다는 새로운 문제점이 발생됐다. 그림 2는 *firstmix*의 구성 및 구성요소들의 기능과 상대적인 부하 정도를 표현한다.

3. 제안하는 방법

이 장에서는 여러 번의 암호화 작업에 따른 송신자의 과도한 부하문제와 *firstmix*의 익명성 보장문제에 대한 해결방법으로서 송신자의 부하를 믹스 네트워크를 구성하는 일련의 믹스 노드들에게 분배함으로서 부하를 줄이고 안전하게 익명성을 제공할 수 있는 방법을 제안하고 제안하는 방법이 적용된 믹스 시스템에서 이루어지는 메시지 전송 프로토콜을 정의한다.

3.1. 송신자의 부하 분담 - 중계 믹스 노드



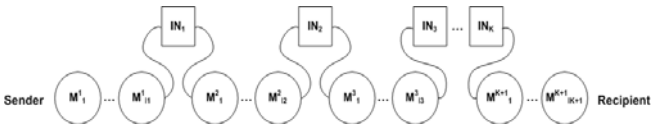
(그림 3) 중계 믹스 노드의 중첩 암호화 분산

송신자 부하의 주원인은 전송할 메시지들을 전송경로에 포함되는 믹스 노드들의 공개키로 여러 번 암호화 하는데 있다. 따라서 송신자 부하를 줄이기 위해서는 보안상 문제가 되지 않는 범위 내에서 암호화 작업을 믹스 네트워크를 구성하는 일련의 믹스 노드들에게 분배하는 것이 필요하며, 우리는 송신자의 부하를 분배받은 믹스 노드들을 '중계 믹스 노드'라고 정의했다. 그림 3은 믹스넷과 중계 믹스 노드가 적용된 부하분산 믹스(Load balanced Mix, 이후 L-믹스라 호칭한다.)에서 메시지 암호화와 암호화된 메시지의 전송과정을 비교해서 보여준다. L-믹스에서 첫 번째와 세 번째에 위치한 믹스 노드가 바로 중계 믹스 노드이며 송신자의 암호화 작업이 각각의 중계 믹스 노드로 나뉘는 것을 볼 수 있다.

중계 믹스 노드와 그 수는 메시지 전송이 이루어지기 이전인 전송할 메시지들의 전송경로를 선택하는 단계에서 결정된다. 만약 중계 믹스 노드가 한 개이면서 동시에 송신자와 인접해 있다면 *firstmix*와 동일하며 모든 믹스 노드가 중계 믹스 노드로 이루어져 있다면 믹스넷과 동일하다. 송신자는 믹스 노드와 중계 믹스 노드를 구분하기 위해 전송할 메시지에 플래그 비트(flag bit)를 첨부하고 암호화한 뒤 이를 믹스 네트워크로 전송한다. 이후 전송경로에 포함된 각 믹스 노드들은 해당 메시지를 복호화하고 플래그 비트 값에 따라 자신이 믹스 노드인지 중계 믹스 노드인지 파악한다.

3.2. L-믹스 시스템의 구성

L-믹스는 그림 4와 같이 기존의 믹스 시스템에 중계 믹스 노드가 추가된 형태로 송수신자, 믹스 노드, 중계 믹스 노드로 이루어져있다.



(그림 4) L-믹스의 네트워크 구성

3.3. 프로토콜의 요구사항

프로토콜을 실현하는데 필요한 요구사항은 다음과 같다.

- 송신자는 믹스 네트워크를 구성하는 일련의 믹스 노드들 중에서 몇 개의 중계 믹스 노드를 선택할 수 있다.
- 송신자는 송수신자와 중계 믹스 노드 사이, 중계 믹스 노드들 사이에 각각 존재하는 믹스 노드의 수를 결정할 수 있다.
- 모든 중계 믹스 노드들은 동일한 기능을 수행한다.

3.4. 메시지 전송 프로토콜

프로토콜을 기술하는데 필요한 용어를 다음과 같이 정의하고 노드별 프로토콜에 대해 살펴본다.

- MSG – 전달하고자 하는 원본 메시지
- R_i – i번째 수신자
- M^R_n – IN^{R-1}과 IN^R 사이 n번째 믹스 노드
- IN_K – k번째 중계 믹스 노드
- NTF – 믹스 노드와 중계 믹스 노드를 구별 해주는 노드 타입 플래그(Node Type Flag) 비트
- P_A – A의 공개키
- R_A – A의 비밀키
- l_n – 송수신자와 중계 믹스 노드 사이, 중계 믹스 노드들 사이의 믹스 노드의 믹스 노드의 수
- $E_{PA}[MSG]$ – A의 공개키로 암호화된 메시지
- A -> B : MSG – A가 MSG를 B에게 전송

3.4.1. 송신자

송신자의 동작은 모두 여섯 단계로 이루어지며 각 단계는 다음과 같다.

1) n개의 믹스 노드들 중에서 k개의 중계 믹스 노드를 선택하고 그들 간 전송경로를 결정한다.
2) 'MSG'를 수신자의 공개키로 암호화하여 아래와 같은 암호화된 메시지를 생성한다.
   - $E_{PRi}[MSG]$
3) '2)'에서 생성한 메시지에 노드타입, 다음 전송경로, 다음 전송경로까지의 믹스 노드 수를 차례대로 포함하여 IN_K의 공개키로 다시 암호화해서 아래와 같은 메시지를 생성한다. 이렇게 함으로서 IN_K는 자신의 개인키로 메시지를 복화화 했을 때 다음 전송경로를 알 수 있고 해당 노드로 메시지를 전송 할 수 있다.
   - $E_{PINK}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]]$
4) '3)'의 결과 생성된 메시지를 IN_1에 대해서까지 암호화한다. 이 결과 생성된 암호화된 메시지는 다음과 같다(이후부터 이 메시지를 MSG'라 표기한다.).
   - $E_{PIN1}[NTF, IN_2, l_1, E_{PIN2}[NTF, IN_3, l_2, E_{PIN3}[.... E_{PINk}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]] ...]]]$
5) IN_1에 이르는 전송경로를 결정하고 경로에 포함된 믹스 노드들의 공개키로 MSG'을 차례대로 암호화하여 최종적으로 전송할 메시지를 생성한다.
   - $E_{PM11}[M^1_2, E_{PM12}[... E_{PM1l1}[MSG'] ...]]$
6) '5)'의 결과를 첫 번째 믹스 노드에 전송한다.
   - Sender → M^1_1 : $E_{PM11}[M^1_2, E_{PM12}[... E_{PM1l1}[MSG'] ...]]$

3.4.2. 중계 믹스 노드

중계 믹스 노드의 동작은 모두 네 단계로 이루어지며 각 단계는 다음과 같다.

1) 수신된 메시지를 복호화해서 노드타입, 다음 전송경로, 다음 전송경로까지의 믹스 노드 수, 다음 경로의 공개키로 암호화된 메시지를 얻는다.
   - NTF, IN_{n+1}, l_1, $E_{PINn+1}[NTF, IN_{n+2}, l_2, E_{PINn+2}[.... E_{PINk}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]] ...]]$
2) 노드 타입 플래그를 통해 자신을 확인하고 다음 중계 믹스 노드에 이르는 l_n의 길이를 갖는 전송경로를 설정한다.
3) '2)'에서 설정한 전송경로에 포함되는 믹스 노드들의 공개키로 메시지를 중첩 암호화하여 다음과 같은 메시지를 생성한다(이후부터 이 메시지를 MSG''라 표기한다.).
   - $E_{PMR1}[M^R_2, E_{PMR2}[... E_{PINn+1}[NTF, IN_{n+2}, l_2, E_{PINn+2}[.... E_{PINk}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]] ...]] ...]]$
4) 이 결과를 믹스 노드에 전송한다.
   - Sender → M^R_1 : MSG''

3.4.3. 믹스 노드

믹스 노드의 동작은 모두 두 단계로 이루어지며 각 단계는 다음과 같다.

1) 수신된 메시지를 복호화해서 다음 노드에 대한 정보와 다음 노드의 공개키로 암호화된 메시지를 얻는다.
   - M^R_n, $E_{PMRn+1}[... E_{PIN2}[NTF, IN_3, l_2, E_{PIN3}[.... E_{PINk}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]] ...]] ...]$
2) 다음 믹스 노드의 공개키로 암호화된 메시지를 해당 노드에 전송한다.
   - M^R_n → M^R_{n+1}: $E_{PMRn+1}[... E_{PIN2}[NTF, IN_3, l_2, E_{PIN3}[.... E_{PINk}[NTF, R_i, l_{K+1}, E_{PRi}[MSG]] ...]] ...]]$

3.4.4. 수신자

마지막 중계 믹스 노드로부터 전송된 메시지를 수신자의 개인키로 복호화해서 MSG를 수신한다.

4. L-믹스의 특성

이 장에서는 L-믹스가 송신자 부하분산과 익명성 보장에 어떤 특성을 갖는지를 믹스넷 및 *firstmix*와 비교한다.

4.1. 송신자 부하분산

다음은 L-믹스와 비교대상 시스템들 간의 송신자 및 노드별 부하비교 내용이다.

4.1.1. 가정

- 가정 1. 송신자 부하에 영향을 끼치는 요소로 암호화 외에 다른 요소는 고려하지 않는다.
- 가정 2. 각 시스템들(믹스넷, *firstmix*, L-믹스)에서 사용되는 총 믹스 노드의 수는 동일하다.
- 가정 3. 각 시스템들에서 사용되는 송신 디바이스 및 믹스 노드들은 동일한 성능을 가진다.

4.1.2. 용어 정의

- n – 전송경로에 포함되는 모든 믹스 노드의 수
- L – 메시지를 한번 암호화 하는데 따른 부하량

4.1.3. 시스템별 부하량

1) 믹스넷

송신자는 메시지를 수신자의 공개키로 먼저 한 번 암호화한 후, 암호화된 메시지를 전송경로 상에 있는 믹스 노드들의 공개키로 다시 암호화한다. 따라서 총 암호화 횟수는 믹스 노드 수와 수신자 수의 합인 n+1이므로 송신자의 총 부하량은 (n+1)L이다.

2) *firstmix*

초기의 *firstmix*는 송신자가 메시지를 첫 번째 믹스 노드의 공개키로 암호화 하지 않고 첫 번째 믹스 노드에게 곧바로 전달한다. 하지만 공격자가 암호화가 되지 않은 메시지를 중간에서 가로채는 경우, 해당 메시지의 내용을 알 수 있다. 따라서 본 논문에서는 전달되는 모든 메시지는 해당 노드의

공개키로 암호화되어 전송된다고 가정하고 이 가정에 따라 송신자는 첫 번째 믹스 노드의 공개키로 한번 암호화한다. 이 경우 송신자의 부하량은 L이다.

첫 번째 믹스 노드는 송신자를 대신해서 전송경로를 결정하고 전송경로에 포함되는 믹스 노드들의 수만큼 암호화한다. 따라서 총 암호화 횟수는 총 믹스 노드의 수에서 자신을 뺀 수와 수신자 수를 더한 수의 합인 n이므로 첫 번째 믹스 노드의 부하량은 nL이다.

3) L-믹스

L-Mix에서 송신자는 전송하려는 메시지를 수신자의 공개키로 암호화 한 후, 전송과정을 통해 경유하게 될 중계 믹스 노드의 공개키로 다시 한 번 암호화한다. 이때 송신자와 첫 번째 중계 믹스 노드 사이에 믹스 노드들을 두고자 한다면 해당 믹스 노드의 수만큼 다시 암호화한다. 따라서 총 암호화 횟수는 수신자, 중계 믹스 노드 그리고 수신자와 첫 번째 중계 믹스 노드 사이의 믹스 노드 수의 합인 $K+1+l_1$이므로 송신자의 부하는 $(K+1+l_1)L$이다.

첫 번째 중계 믹스 노드는 두 번째 중계 믹스 노드에 이르는 전송경로를 결정하고 경로에 포함된 믹스 노드의 수만큼 암호화 하게 된다. 따라서 총 암호화 횟수는 첫 번째와 두 번째 중계 믹스 노드 사이의 믹스 노드 수의 합이므로 첫 번째 중계 믹스 노드의 부하는 $(l_1)L$이다. 나머지 중계 믹스 노드들의 부하 역시 이와 같은 방법으로 계산될 수 있으며 이것을 일반화 시켰을 때, K번째 중계 믹스 노드의 부하는 $(l_{K+1})L$이다.

4.1.4. 시스템 간 비교

각 시스템의 노드별 부하는 표 2와 같으며 송신자 부하와 네트워크에 대한 송신자 부하분산 정도에 대한 비교는 다음과 같다.

<표 2> 각 시스템의 노드별 부하

System / Node	Mix-net	*firstmix*	L-Mix
Sender	(n+1)L	L	$(K+1+l_1)L$
First Intermediate Mix Node (First Mix Node)	•	{(n-1)+1}L	$(l_2)L$
Second Intermediate Mix Node	•	•	$(l_3)L$
⋮	⋮	⋮	⋮
Total Load	(n+1)L		

1) 송신자 부하

각 시스템별 송신자 부하량은 아래와 같이 비교된다.

$$firstmix \leqq \text{L-Mix} \leqq \text{Mix-net}$$

*firstmix*의 경우, 송신자는 수신자의 공개키로 한 번 암호화 하는 것 외에 송신자의 모든 암호화 작업을 첫 번째 믹스 노드가 대신하게 함으로서 송신자의 부하는 가장 적다. 이에 반해 L-믹스의 경우, 송신자는 수신자의 공개키로 암호화 하는 것 외에 중계 믹스 노드 간 경로를 설정하기 위해 중계 믹스 노드의 수만큼 암호화를 하기 때문에 부하는 *firstmix*와 같거나 많을 수 있다(*firstmix*와 송신자 부하가 같은 경우는 중계 믹스 노드가 한 개이면서 송신자와 인접한 경우이다.). 따라서 중계 믹스 노드의 수에 따라 믹스넷 보다 크거나 같고 *firstmix* 보다 작거나 같은 범위 안에서 송신자 부하의 분배효과를 가진다.

2) 네트워크에 대한 송신자 부하분산 정도

각 시스템별 네트워크에 대한 송신자 부하분산 정도는 아래와 같이 비교된다.

$$\text{Mix-net} < firstmix \leqq \text{L-Mix}$$

*firstmix*에서는 믹스 노드들 중에서 오직 첫 번째 믹스 노드만 송신자의 부하를 나눠 갖는 반면 L-믹스에서는 중계 믹스 노드의 수만큼 송신자의 부하가 나뉨으로서 네트워크 전체에 걸쳐 송신자의 부하가 골고루 분배된다. 만약 중계 믹스 노드의 수가 한 개이며 송신자와 인접해 있다면 *firstmix*와 같은 성능을 보인다.

4.2. 익명성 보장

각 시스템별 익명성 보장정도는 아래와 같이 비교된다.

$$firstmix \leqq \text{L-Mix} \leqq \text{Mix-net}$$

믹스넷에서는 모든 믹스 노드가 공격자에 의해 공격당해야만 메시지의 송신자와 수신자가 밝혀지기 때문에 익명성을 보장하지 못하므로 가장 안전하고, *firstmix*에서는 첫 번째 믹스 노드가 송수신자 모두를 알고 있기 때문에 오직 첫 번째 믹스 노드 하나만 공격당한다면 익명성을 보장할 수 없으므로 가장 안전하지 못하다. 반면 L-믹스는 모든 중계 믹스 노드가 공격당해야만 익명성을 보장할 수 없는데, 중계 믹스 노드의 수는 사용자가 설정할 수 있으므로 *firstmix* 보다 크거나 같고 믹스넷 보다 작거나 같은 범위 안에서 *firstmix*와 같은 정도의 익명성 보장을 할 수 있고 믹스넷과 같은 정도의 익명성 보장을 할 수 있다.

5. 결 론

본 논문에서는 익명통신을 제공하는데 있어서 송신자의 과도한 부하문제를 해결하는 방법으로서 L-믹스를 제안하고 여기에 필요한 메시지 전송 프로토콜을 정의한 후, 그 특징들을 비교분석했다. 제안한 방법을 통해 저성능의 송신 디바이스를 사용하는 사용자들은 서비스의 종류에 따라 메시지를 암호화하는데 많은 시간이 소요되어 해당 서비스를 제공받는데 지체되거나 서비스를 제공받지 못할 수 있는 문제를 해결할 수 있을 것이다.

참고문헌

[1] G. Danezis. Better Anonymous Communications. PhD thesis, University of Cambridge, Computer Laboratory, 2004.
[2] D. Chaum, “"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,"” Communications of the ACM, v.24, n. 2, pp. 84-88, Feb 1981.
[3] Emin Islam Tatlı, Dirk Stegemann, and Stefan Lucks, "Dynamic Mobile Anonymity With Mixing", Transactions On Engineering, Computing And Technology, v.6, pp.83-89, June 2005.
[4] Emin Islam Tatlı, Dirk Stegemann, and Stefan Lucks, "Dynamic Anonymity", Transactions On Engineering, Computing And Technolog, v.6, pp.83-89, June 2005.
[5] Claudia Díaz, Bart Preneel “Taxonomy of Mixes and Dummy Traffic”, International Information Security Workshops 2004, pp.215-230, 2004.