모빌 IP의 인증 프로토콜과 익명성 지원을 위한 RC5 알고리즘의 하드웨어 구현

°김 기준, 채 수환, 박 종서, 염 동복
한국항공대학교 컴퓨터공학과

Hardware Implementation of RC5 algorithm for Authentication Protocol and Anonymity in Mobile IP

KiJun Kim, SooHoan Chae, JongSou Park, DongBok Yeom
Dept. of Computer Engineering, Hankuk Aviation University

요 약

모빌 IP는 이동 노드의 모든 메시지를 중계하는 외부 에이전트에 대한 인증 기능이 없으며 이동 노드의 익명성을 제공하지 않는다 이로 인하여 도청과 같은 수동적 공격에 취약하며 또한 스무스 핸드오프를 위한 이동 노드와 외부 에이전트간의 등록 키 공유문제가 발생한다 본 논문에서는 외부 에이전트와 홈 에이전트 간에 추가적인 부하를 최소화시킬 수 있는 형태의 인증 및 키 분배 프로토콜과 익명성 제공 방법을 제안하고 추가적인 시간소모를 최소화하기 위하여 암호화 알고리즘을 VHDL을 통하여 하드웨어로 설계하였다.

1. 서 론

인터넷 이용의 급증에 따른 데이터 통신량의 증가로 미국에서는 99년, 일본에서는 2002년이면 데이터 통신량이 음성통신량을 앞지를 것으로 예측되고 있다.[1] 따라서 이동통신 시장에서도 데이터 통신 서비스의 비중이 기존의 음성통신을 능가하게 될 것이다.

시장조사 기관인 세미코사는 2003년에는 모빌 컴퓨팅 시장이 75억 달러에 달할 것으로 예측하면서, 수요 증대의 가장 큰 요인으로 인터넷을 통한 기업 네트워크 접속 요구증대로 분석하였다. 그러나 가상 사설망을 이용한 익스트라넷(extranet)으로 발전하고 있는 기업 네트워킹에서도 원격 접속(*remote access*)의 보안기반은 취약하다. 따라서 모빌 IP가 단순한 홈 에이전트(HA)뿐 아니라 실제 기업 네트워크가 홈 네트워크인 경우를 지원할 수 있어야 한다.

그러나 현재의 모빌 IP 표준안에서는 그림 1과 같이 이동 노드(MN)로 들어오고 나가는 모든 데이터를 중계하는 외부 에이전트(FA)에 대한 인증 없이 MN와 FA간에 스무스 핸드오프를 위한 등록 키(registration key)의 공유가 필요하다는 점, 익명성을 지원하지 않는다는 점 등 여러 가지 보안 문제점들이 있다 [2]

본 논문에서는 모빌 IP 시스템에서 FA와 HA간에 인증 및 등록 키(registration key)를 분배하기 위한 프로토콜과 익명성지원을 제안하였다. 이어 제안된 프로토콜을 BAN logic을 이용하여 검증하고 replay 공격에 대한 안전성을 검토하였고 [3],[4] 제안된 인증 및 키 분배 프로토콜과 익명성의 핵심이

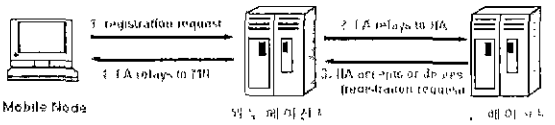

그림 1. 모빌 IP의 이동 노드 등록

되는 암호화 알고리즘을 표준 하드웨어 기술 언어인 VHDL(Very high speed integrated circuit Hardware Description Language)를 이용하여 하드웨어로 구현하였다

2. 모빌 IP 시스템의 보안 향상

2.1. 인증 및 키 분배 프로토콜

정보 보호의 기본요소는 인증과 암호화이다. 통신하려는 상대의 실체를 확인하는 인증을 통하여 스푸핑, replay, 서비스 거부 등의 능동공격에 대처하고 암호화를 통하여 도청 등의 수동공격에 대처할 수 있다. 인증 및 키 분배 프로토콜은 암호화에 의한 보안에 필수적인 키 분배를 위한 인증 문제를 해결하기 위한 것으로 보안 프로토콜의 기본이 되며 Needham-Schroeder 프로토콜을 시작으로 DASS, Keberos등 환경에 따라 많은 인증 및 키 분배 프로토콜들이 제시되었다.[5]

모빌 IP의 스무스 핸드오프를 위한 등록 키 분배 문제에 있어서도 *Diffie-Hellman, 공개키 인증서*를 이용하는 방법과 MN과 FA간 또는 FA와 HA간에 SA(security association)을 설정하는

방법 등이 제시되었다. 그러나 Diffie-Hellman이나 공개키 인증서는 키 관리상의 어려움 없이 키를 분배할 수 있을 뿐으로 공개키 암호 시스템에서도 안전한 키 분배를 위해서는 공개키 인증기관과의 인증 및 키 분배 프로토콜이 요구된다. 또한 SA를 설정할 경우 대상이 m, n개라면 2mn개의 SA가 사전에 설정되어야 한다는 점에서 비효율적이다.[6],[7] 본 논문에서는 적은 부하로 모빌IP의 이동성 지원 목표를 달성하는 것을 목적으로 인증 서버 AS를 추가하여 random발생시킨 nonces를 이용, 메시지의 freshness를 검증하고 인증을 수행하는 프로토콜을 그림2와 같이 설계하였다.

1 $FA \rightarrow HA : \{FA+I,\ N_{FA}\}K_{FS}$

2. $HA \rightarrow AS : \{FA+I,\ N_{FA}\}K_{FS},\ \{HA+J,\ N_{HA}\}K_{HS}$

3. $AS \rightarrow HA : \{K,\ N_{HA},\ N_{FA}\}K_{FS},\ \{K,\ N_{HA}\}K_{HS}$

4 $HA \rightarrow FA : \{K,\ N_{HA},\ N_{FA}\}K_{FS},\ N_{HA}$

그림 2. 제안된 인증 및 키 분배 프로토콜

프로토콜이 실행되면 FA는 이번 인증 요구에 사용할 자신의 id인 FA와 random생성한 nonces N_{FA}를 AS와의 비밀키인 K_{FS}로 암호화하여 HA에 전송한다. HA도 동일한 형태의 메시지를 생성하여 FA의 메시지와 함께 AS에 전송한다. AS가 HA, FA간 등록 키를 선택한 후 nonces들과 조합하고 FA, HA와의 비밀키로 암호화하여 송신하면 이를 수신한 HA, FA는 서로 인증된다.

다음으로 인증 및 키 분배 프로토콜의 흐름상의 오류를 밝혀내는 데 유용하여 Keberos를 비롯한 많은 프로토콜들의 검증에 채택된 BAN logic을 이용하여 검증하였다.[5] BAN logic은 프로토콜을 idealized protocol로 변환하여 assumption들을 정리한 뒤 assumption들이 충족되는 지를 분석하는 과정으로 이루어진다.[3] 제안된 프로토콜의 idealized protocol과 중요한 assumption들을 그림 3, 4에 제시하였다.

Message 1. $FA \rightarrow HA : \{\langle FA\rangle_I, N_{HA}\}K_{FS}$

Messaeg 2. $HA \rightarrow AS \quad \{\langle FA\rangle_I, N_{FA}\}K_{FS},\ \{\langle HA\rangle_J, N_{HA}\}K_{HS}$

Message 3. $AS \rightarrow HA$:

$\left\{HA \overset{K}{\Longleftrightarrow} FA, \#(HA \overset{K}{\Longleftrightarrow} FA), N_{HA}, N_{FA}, HA|\sim N_{HA}\right\}K_{FS}$,

$\left\{HA \overset{K}{\Longleftrightarrow} FA, N_{HA}\right\}K_{HS}$

Message 4. $AS \rightarrow HA$:

$\left\{HA \overset{K}{\Longleftrightarrow} FA, \#(HA \overset{K}{\Longleftrightarrow} FA), N_{HA}, N_{FA}, HA|\sim N_{HA}\right\}K_{FS}, N_{HA}$

그림3. Idealized Protocol

$AS \models \#(N_{HA})$, $AS \models HA \sim \#(N_{FA})$

$HA \models (AS \Rightarrow HA \overset{K}{\Longleftrightarrow} AS)$, $FA \models (AS \Rightarrow FA \overset{K}{\Longleftrightarrow} AS)$

$FA \models (AS \Rightarrow \#(FA \overset{K}{\Longleftrightarrow} HA))$, $HA \models (AS \Rightarrow \#(FA \sim N_{FA}))$

$FA \models (HA \Rightarrow AS \models \#(FA \overset{K}{\Longleftrightarrow} HA))$

그림 4. 제안된 프로토콜의 assumption

제안된 프로토콜의 assumption들을 충족시키기 위한 핵심은 우선 AS가 HA, FA의 메시지를 수신했을 때 nonces의 freshness를 확인할 수 있어야 한다는 점이며 두번째로 등록키를 포함한 메시지를 중계 받는 FA가 HA에 비해 보안상 불리한 위치에 속한다는 점이다. 제안된 프로토콜에서는 HA, FA의 이전 인증 요구의 id와 인증 요구횟수인 I, J를 더한 값을 이번 인증 요구의 id로 사용함으로써 AS가 nonces의 freshness를 확인할 수 있게 하였다. 또한 HA는 자신의 nonces인 N_{HA}를 FA로의 AS의 메시지와 함께 FA로 전송한다. 두 개의 메시지를 수신한 FA는 먼저 AS로부터의 메시지를 복원하여 세션키 K와 N_{HA}를 얻는다. nonce 검증을 통해 AS 인증, 세션 키 생성, K의 freshness를 확인할 수 있으며 HA로부터의 N_{HA}와 비교하여 HA를 인증하고 세션 키를 속이지 않았다는 사실을 확인함으로써 HA를 위장한 공격에 대처할 수 있다.

프로토콜의 한 인스턴스에서 정보를 빼내 다른 인스턴스의 등록 메시지에 사용하는 interleaving등의 replay 공격은 방법이 다양하고 일반적인 검증 수단과 대책이 존재하지 않으므로[4] 프로토콜의 전반부에서 HA, FA의 메시지를 암호화하는 방식으로 대처하였다.

제안된 프로토콜은 FA와 HA간의 인증을 위하여 AS를 추가하였으며 시간 소요를 줄이기 위하여 MN의 등록 메시지를 처리하는 과정에서 HA, AS간에 한 번의 메시지 교환의 추가로 전체 동작이 종료된다 이후 HA는 키 분배 센터(KDC)로써 스무스 핸드오프를 지원할 수 있다.

2.2. 사용자 익명성

이동 컴퓨팅 환경에서 이동 호스트의 신원과 행적을 보호하는 익명성과 추적 불가능성의 제공 또한 중요하다. 기밀성을 보장하기 위한 대책들이 사용기법과 요구되는 보안강도의 다양성으로 인하여 하부통신구조에 대하여 많은 가정을 하고 있기 때문에 사용자의 접근성을 보장하면서 기밀성과 결합하여 익명성을 제공하면 보안의 정도를 높일 수 있다. 익명성은 C1 레벨의 도청자로 부터 사용자 신원 은폐로부터 C5 레벨의 홈 네트워크로부터 사용자 행동 은폐로 분류되며[8] 현재 중요시되는 익명성 대책들은 주로 GSM의 TMSI와 같이 불법적인 도청자가 사용자의 현재 위치와 실제 신원간의 연관성을 유추해내지 못하게 하기 위하여 시간의 경과나 접속횟수에 따라 매 세션마다 다른 가명(alias)를 부여하는 C1 레벨이다. 제안된 방법들은 주로 쌍방간에 약속된 일 방향 함수를 이용하여 일정한 시간 간격을 두고 사용자와 인증 서버가 가명을 갱신해 나가는 방법이다. 그러나, 사용자와 인증 서버간의 시간 동기화는 어렵기 때문에 초나 분 단위가 아닌 몇 시간을 단위로 가명이 갱신된다 이러한 취약성과 함께 시간 동기가 정확하게 맞지 않을 경우 가명동기화가 상실될 수 있기 때문에 가명동기를 복구할 수 있는 기법이 또한 요구된다. 따라서, one time password 시스템과 유사하게 이동 노드의 HA에 대한 등록 요구(registration request) 메시지마다 가명

HA에 대한 등록 요구(registration request) 메시지마다 가명을 갱신하는 시스템이 보다 효율적이다. 즉, 마지막으로 사용된 등록 요구 메시지의 가명과 접속횟수 j를 가지고 계산한 $Alias_{i+1} = f_K(Alias_i, j)$를 다음 등록 요구의 가명으로 사용하는 방식이다. 등록 요구에 따른 가명갱신 방식은 시간동기 가명방식보다 등록 요구 당 연산량은 증가하지만 시간동기 방식의 경우 일정시간마다 모든 가명을 한꺼번에 갱신해야 하며 접속요구를 자주 하지 않는 이동 노드의 경우에도 가명갱신이 수행되어야 한다는 점에서 이점을 가진다. 그러나 등록 요구가 급증할 경우 HA측에 많은 연산이 요구됨으로 일방향 함수 f_K의 선택이 중요하고 신뢰성 있는 처리를 위해서는 하드웨어 구현이 필요하다. 주로 사용되는 일 방향 함수인 MD5는 구조상 병렬처리가 어려워 하드웨어로 구현하더라도 큰 성능향상을 기대할 수 없기 때문에 네트워크의 고속화에 따라 AHA나 bucket hash와 같은 대안들이 연구되고 있지만 대안들의 안정성이 확인되지 않은 현재에는 RC5와 같이 64비트의 암호화 알고리즘을 CBC(Cipher Block Chaining) 모드로 사용함으로써 보다 빠르게 수행될 수 있다.

3. 하드웨어 구현

모빌 IP의 요구 조건인 초당 1회의 이동성을 지원하기 위해서는 HA, FA간의 인증 및 키 분배에 소모되는 시간을 최소화하기 위하여 하드웨어로 구현되는 것이 바람직하다. 모빌 IP는 인증 과정 후 HA, FA간에 추가적인 암호화가 필요하지 않고 MN, HA, FA 모두 자신의 비밀키만을 사용한다. 따라서 암호화 알고리즘은 64비트 암호화이상의 강도를 가지며 짧은 메시지의 암호화에 적합하여야 한다. 본 논문에서 제안한 프로토콜과 익명성은 암호화 알고리즘의 반복 수행에 중점을 두어 적절한 암호화 알고리즘의 하드웨어 구현으로 빠른 수행이 가능하도록 설계되었다. 표준으로 사용되던 56비트 DES의 공격이 성공하고 최근에는 중요정보에 대해서는 96비트 이상 암호화의 필요성이 제기되고 있지만 이동 통신의 경우 64비트 암호화가 적절한 것으로 판단된다. 암호화 알고리즘으로는 구성 함수가 간단하여 게이트 양이 적고 취약키가 존재하지 않는 64비트 암호화 기법인 RSA사의 RC5를 선택하여 속도면 보다 크기를 줄이는 것을 목표로 설계하였다.

RC5 알고리즘은 사용자의 비밀키를 바이트 단위로 배열L에 넣은 뒤 매직 상수를 이용하여 덧셈연산에 의해 계산된 배열 S와 섞는 키 확장 과정을 통하여 일 방향성을 얻는다. 또한 RC5는 하나의 입력블록에 대한 암·복호화 수행보다 키 확장과정의 수행시간이 더 걸리기 때문에 키 확장부와 암·복호화부를 분리하여 S[0], S[1]의 값이 출력되면 암호화가 시작될 수 있도록 설계하였으며 이중 암호화 부의 구조를 보면 그림 5와 같고 그림6은 평문을 암호화하는 과정을 모의 실험한 결과이다.

설계된 RC5는 키 확장에 408클락, 16라운드 수행에는 132클럭이 소요되며 함께 수행할 경우 432클럭에 64비트 입력블록을 암호화할 수 있다. 암·복호화 부만을 볼 경우 RC5를 구성하는 기본 기능인 XOR, Rotate, Add와 입력을 선택하기 위한 멀티플렉서만으로 구성하여 크기의 소형화를 꾀하였다.

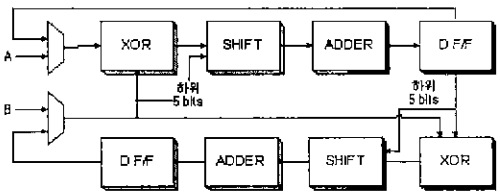

그림 5 . RC5 블록도

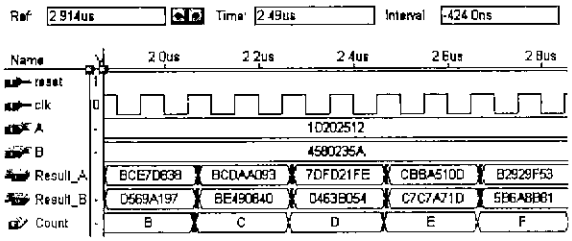

그림 6 . 암호화 모의 실험 결과

4. 결 론

본 논문에서는 모빌 IP가 기업 네트워크 환경을 지원하기 위하여 필수적인 인증 및 등록 키 분배 프로토콜과 익명성을 제공하는 방법을 제안하고 핵심 요소인 RC5 암호화 알고리즘을 하드웨어로 구현하였다. 사용자 인증 뿐 아니라 메시지 인증을 수행할 수 있도록 고속 인증 알고리즘의 설계 및 하드웨어 구현을 위한 연구를 지속할 것이다.

참 고 문 헌

[1] 전 홍범, "High speed network solution for internet", KRNET 98, June 1998

[2] C. Perkins, "IP Mobility Support", RFC 2002, October 1996

[3] M. Burrow et al.,"A Logic of Authentication", ACM Transactions on Computer System, v.8, n.1, Feb 1990

[4] P. Syverson, "A Taxonomy of Replay attacks," Proceedings of the Computer Security Foundations Workshop VII, Franconia NH, 1994

[5] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, 1996

[6] C. Perkins., "Route Optimization in Mobile IP", Internet draft, July 1998

[7] S. Mocas and T. Schubert, "Formal Analysis of IP Layer Security" DIMACS Workshop on Design and Formal Verification of Security Protocols, September 1997

[8] N. Asokan et al., "Anonymity and Untraceability in a Mobile Networks", Proceedings of the ACM International Conference on Mobile Computing and Networking, Dec. 1994