검증자 기반 Ad-hoc 보안 인증기법

이철승[*] · 홍성표[**] · 이호영[***] ·이준[****]

[*]조선대학교 대학원 컴퓨터공학과

[**]조선대학교 전자정보공과대학 정보통신공학과

[***]초당대학교 정보통신공학과

[****]조선대학교 전자정보공과대학 컴퓨터공학과

Ad-hoc Security Authentication Technique based on Verifier

Cheol-seung Lee[*] · Seong-pyo Hong[**] · Ho-young Lee[***] · Joon Lee[****]

[*]Dept. of Computer Engineering, Graduate School, Chosun University

[***]Dept. of Information&Communication Engineering, Chosun University

[***]Dept. of Information&Telecommunications Engineering, Chodang University

[****]Dept. of Computer Engineering, Chosun University

E-mail : cyberec@chosun.ac.kr

요 약

본 논문은 Ad-hoc 네트워크의 무선 보안의 취약성과 현재 활용되고 있는 인증기법을 분석하여, Ad-hoc 기반 강력한 인증을 위해 검증자를 이용한 인증기법을 제안한다. 제안기법은 라우팅, 등록, 실행 단계로 구성하며, 라우팅 단계에서는 AODV 프로토콜을 이용하였다. 등록 및 실행 단계에서는 적법한 소스노드 인증을 위해 원타임 패스워드 S/key와 패스워드 기반 DH-EKE를 적용하였다. 제안 인증 기법의 안전한 패킷 데이터 전송과 데이터 암호화를 위한 세션키 설정시 *H(pwd)* 검증자로 암호화 하여 키교환을 수행하고, 원타임 패스워드는 소스노드의 패스워드 소유 검증과 효율성 향상을 위해 사용한다. EKE는 식별자를 해쉬함수에 모듈라 지수승 하는 DH-EKE 방식을 이용하여 단대단 세션키를 설정하고 키교환 단계에서는 *H(pwd)* 검증자로 암호화 함으로써 안전한 세션키 교환을 한다.

ABSTRACT

This paper suggests One-time Password key exchange authentication technique for a strong authentication based on Ad-hoc Networks and through identify wireless environment security vulnerabilities, analyzes current authentication techniques. The suggested authentication technique consists of 3 steps: Routing, Registration, and Running. The Routing step sets a safe route using AODV protocol. The Registration and Running step apply the One-time password S/key and the DH-EKE based on the password, for source node authentication. In setting the Session key for safe packet transmission and data encryption, the suggested authentication technique encrypts message as *H(pwd)* verifiers, performs key exchange and utilizes One time password for the password possession verification and the efficiency enhancement. EKE sets end to end session key using the DH-EKE in which it expounds the identifier to hash function with the modula exponent. A safe session key exchange is possible through encryption of the *H(pwd)* verifier.

키워드

Ad-hoc, AODV, HASH

Ⅰ. 서 론

최근 독립된 네트워크의 구성 및 단말기간의 상호연결 요청으로 Ad-hoc에 관한 연구가 급증하고 있다.

Ad-hoc은 Mn(Mobile node)들이 호스트, 라우

터 기능으로 임베디드 환경에 적합하지만, Mn의 이동성으로 동적 네트워크 토폴로지, 데이터 전송에러, 네트워크 확장성, DOS(Denial of service), 수동·능동적 공격으로 많은 보안상 취약성을 지니고 있다.

본 논문은 보안유지를 위한 가장 기본적이면서도 어려운 측면인 인증기법을 분석하고, 기존 인증기법의 문제점과 안전성 및 효율성을 분석하여 Ad-hoc 기반의 강력한 인증기법을 제안한다.

II. 본 론

2.1 Ad-hoc 라우팅 프로토콜

Ad-hoc은 Table-driven, On-demand, Hybrid 방식의 라우팅 프로토콜로 나눌 수 있으며, 현재 On-demand 방식에 대한 연구가 주류를 이루고 있다. On-demand 방식은 송신할 데이터를 갖는 Sn(Source node)이 Dn(Destination node)의 전송 요구가 있을 때만 즉시, Dn의 경로를 탐색, 생성, 유지하는 방식으로 Table-driven 방식에 비해 제어 트래픽에 의한 오버헤드를 줄일 수 있고, 큰 규모의 네트워크에 적용할 수 있다. [1]

2.2 Ad-hoc OTP S/key

현재 Ad-hoc 인증기법들은 CA(Certificate Authority)의 존재 유·무로 나눌 수 있으며, 무선 네트워크 환경과 Mn의 연산량을 고려할 때 CA가 존재하지 않은 Ad-hoc의 인증기법에 대한 연구가 진행되고 있다.

OTP S/key 인증기법은 독립적(Stand alone) 환경을 위한 인증기법으로 세션키를 사용하는 대표적인 OTP(One time password) 인증기법이다. OTP S/key 기법은 인증시 발생할 수 있는 취약점 및 성능저하를 고려하여 연산과정이 단순하면서도 이동성을 보장해 줄 수 있으며, 안정성과, 실뢰성 및 간편성이 우수하다. Sn에서는 적절한 OTP를 생성되어야 하고, Dn은 OTP를 검증 되어야만 한다.

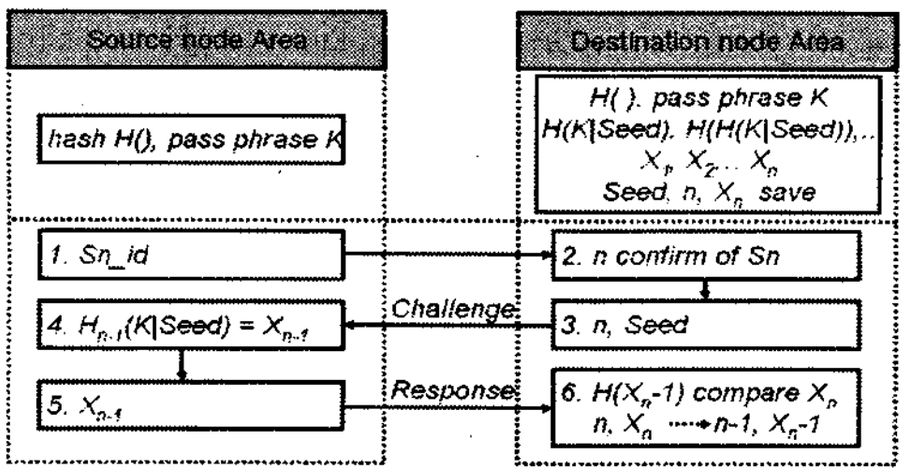

그림 1. 원타임 패스워드 S/Key 방식

2.3 DH-EKE 프로토콜

검증자기반 DH(Diffie Hellman)-EKE(Encrypted Key Exchange) 프로토콜은 송신자가 자신의 패스워드(*pwd*)만을 기억하고, 수신자는 *pwd* 검증자(verifier)만을 저장한다. 검증자는 공격자가 검증자를 소유하고 있더라도 쉽게 *pwd*를 알아내는 것이 불가능 하도록 만들어져야 하며, *H(pwd)*로 만들거나, *pwd* 곱셈근의 원시근 g의 지수로 하여 g^{pwd}로 계산하여 세션키를 분배하는 프로토콜이다. [2]

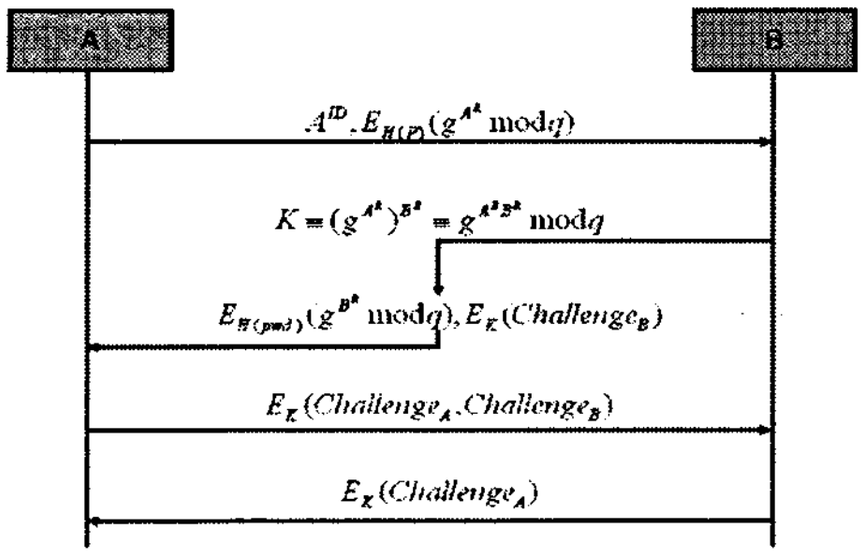

그림 2. 패스워드 기반의 DH-EKE 프로토콜

네트워크 참여자 A는 랜덤수 A^R를 개인키로 선택하여 자신의 ID인 A^{ID}와 참여자 B와 공유된 *H(pwd)*를 이용하여 암호화 한 후 메시지를 B에게 전송한다. B는 *H(pwd)*로 메시지를 복호화한 후 A^R에 B의 랜덤수 B^R을 지수승하여 세션키 K를 구한다. B는 자신의 공개키값 g^{B^R}을 *H(pwd)*로 암호화 하고, $Challenge_B$를 K로 암호화 하여 A에게 전송한다. A는 전송된 메세지를 복호화 하여 g^{B^R}에 A^R을 지수승하여 세션키 $K=g^{B^RA^R}$를 생성하고 이를 이용하여 $Challenge_B$를 복호화 한다. A는 키확인을 위해 자신의 검사값 $Challenge_A$와 $Challenge_B$를 K로 암호화 하여 B에게 전송한다. B는 전송된 메시지를 복호화 하여 B가 소유한 가지고 있는 $Challenge_B$와 A로부터 전송된 $Challenge_B$의 일치여부에 따라 A와 동일한 K를 공유했음을 확인하고, A를 인증한 후 $Challenge_A$를 K로 암호화 하여 전송한다. A는 전송된 $Challenge_A$의 일치여부를 확인한 후 B를 인증한다. [3]

2.4 Ad-hoc OTP S/key 문제점

OTP S/key 기법은 사전공격, 스푸핑, pwd의 사용횟수의 생명주기, 상호인증 불가능등의 문제점이 있으며, 이외에 안전한 Ad-hoc 상호인증을 위해서는 재전송공격, 중간침입자공격(Man-in-the middle attack), Denning-sacco, PFS(perfect forward secrecy), Stolen-verifier 공격에 안전해야 한다.

III. 검증자를 이용한 인증기법

3.1 인증기법 라우팅 단계

Sn이 Dn까지 경로설정을 위해 Nn(Neighbor node)에게 RREQ(Route Request) 패킷을 브로드캐스팅 한다. RREQ 패킷은 루프 방지와 최신의 경로정보를 갖기 위해 Dn의 시퀀스넘버, Sn의 시퀀스넘버와 Sn의 IP주소, 그리고 RREQ를 보낼때마다 증가하는 브로드캐스트 ID가 포함되어 있다. 만일 중간에 위치한 Mn들이 Dn에 대한 경로정보를 가지고 있을때 Dn의 시퀀스넘버가 RREQ에 들어있는 Dn의 시퀀스넘버 보다 크거나 같다면 중간에 위치한 Mn들은 RREQ에 응답할 수 있다. 중간에 위치한 Mn들은 RREQ를 전달하는 과정에서 자신의 라우팅 테이블에 첫 RREQ 패킷을 보내온 Nn의 주소를 기록하며 이렇게 함으로써 역방향 경로를 설정할 수 있다.

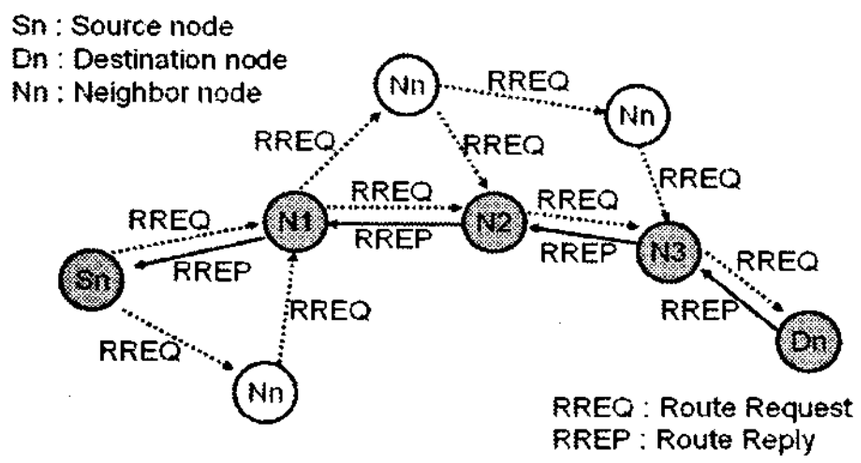

그림 3. AODV 라우팅 단계

RREQ가 Dn에 도착하여 응답을 할 만큼 최근 경로를 가지고 있다면, Dn은 RREP(Route Reply) 메세지를 RREQ의 역방향으로 응답한다. RREP 전송 과정에서 해당 Mn들은 전송경로를 라우팅 테이블에 엔트리로 저장하며, 액티브 상태로 설정하여 양방향 특성의 링크를 지원한다. RREP 메세지를 수신한 Mn은 순방향 경로정보를 생성하여 저장하며 하나의 Mn이 동일한 RREQ 메세지를 중복적으로 수신한 경우 최초로 수신된 것만 사용한다. [4]

3.2 인증기법 등록 단계

등록단계는 Sn과 Dn사이에 확보한 경로를 통해 *Sn_id*와 *MD5*를 *n*번 적용한 검증자 $H^n(pwd)$를 Dn에게 전송한다. Sn은 자신의 *pwd*만 기억하고 Dn은 *Sn_id*, $H^n(pwd)$를 디렉토리에 저장한 후, Dn은 Sn 인증을 위해 공개된 *pwd* $H(g^s)$를 Sn에게 전송한다. $H^n(pwd)$는 OTP S/Key 기법과 동일하게 매 세션마다 $H()$가 하나씩 줄어들기 때문에 $i(i \le i<n)$번째 통신에서는 $H^{n-i+1}(pwd)$와 $H^{n-i}(pwd)$가 검증자로 사용된다. 또한 초기에 설정한 검증자가 *(n-1)*번 사용된 후에는 새로운 *pwd*로 검증자를 만들어 전송한다.

3.3 인증기법 검증 및 실행 단계

3.3.1 검증단계

검증단계는 등록단계에서 전송했던 *Sn_id*와 $H^n(pwd)$를 통해 Dn과 세션키를 공유한다. Sn은 악의적인노드(malicious node)의 공격을 막기위해 $H^{n-1}(pwd)$를 암호화 하여 Dn에게 전송한다. Dn은 Sn으로부터 $H^{n-1}(pwd)$에 $H(H^{n-1}(pwd))$을 적용하여 이미 저장된 $H^n(pwd)$와 같은지를 비교하여 같다면 $H^{n-1}(pwd)$가 제대로 생성되었으며, Sn의 *pwd*를 확인할 수 있다. Dn은 $H^{n-1}(pwd)$을 디렉토리에 저장한 후 *(n-1)*번째 통신까지 동일한 방법으로 검증자를 검증한다.

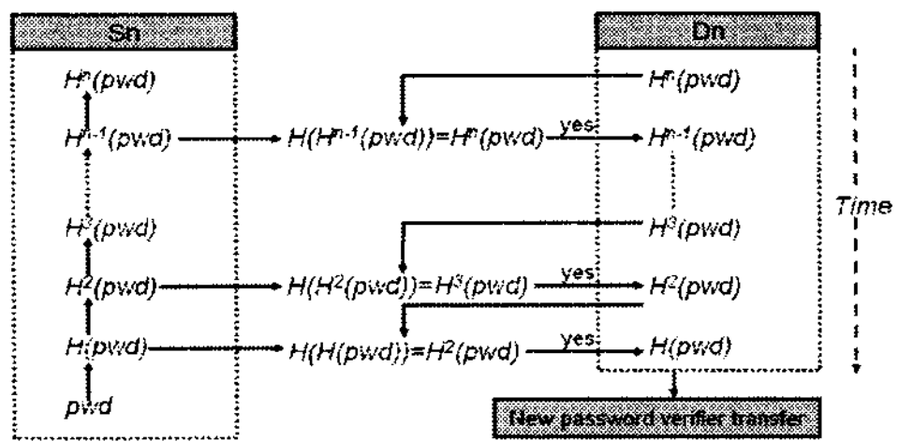

그림 4. 목적지노드 검증 단계

3.3.2 실행단계

실행단계는 제안 인증기법의 *pwd* 키교환의 *i*번째 통신의 단계별 수행과정을 나타낸다. *Sn*은 랜덤하게 생성된 $Sn \in_R [1, q-1]$을 비밀값으로 선택하여 세션키 생성을 위한 키재료값 g^{Sn}를 계산한다. 악의적인노드가 g^{Sn}에 위·변조 공격을 막기 위해 실행단계에서 Sn과 Dn사이에 공유했던 $H^{n-i+1}(pwd)$와 g^{Sn}를 암호화 하여 *Sn_id*와 함께 Dn으로 전송한다. Dn은 Sn으로부터 암호화된 메시지를 받은 후 디렉토리에 저장된 Sn의 *pwd* 검증자를 이용하여 복호화 한다. Dn은 랜덤하게 생성된 $Dn \in_R [1, q-1]$을 비밀값으로 선택하여 세션키 생성을 위한 키재료값 g^{dn}를 계산하고, g^{Sn}에 *Dn*의 지수승 계산을 하여 세션키 $K = g^{SnDn}$을 계산한다. Dn은 장기 비밀키 *s*를 이용하여 다음 통신에 사용할 *pwd* 검증자 $K' = g^{Sns}$를 계산한다.

*K*와 *K'* 생성을 끝낸 Dn은 Sn과 Dn이 생성한 키값의 동일여부를 판별하기 위한 키검증 메시지 $H(K \| K')$를 생성한다. 키 검증 메세지 생성 후 Dn의 장기 공개키 g^s와 악의적인노드가 g^{Dn} 에 위조·변조 공격의 수행을 막기 위해 Dn는 Sn과 비밀리에 공유했던 $H^{n-i+1}(pwd)$로 암호화한 g^{Dn}을 키검증 메세지 $H(K \| K')$함께 Sn에게 전송한다. Sn은 Dn로부터 메세지를 받은 후 자신의 *pwd* 검증자로 복호화하고 Dn의 g^s에 $H()$를 적용하여, 자신이 가지고 있는 공개 *pwd* $H(g^s)$값과 같은지를 비교한다. 만약 일치하지 않는다면 Dn이 올바르지 않은 장기 공개키 값을 전송한 것이므로 Dn과 Sn 사이에 세션을 종료한다. 또한 Dn이 장기 비밀키 *s*를 알고 있음을 *K'*를 사용하여 Dn이 만든 키 검증 메세지를 통하여 검증한다.

본 논문은 Diffie-Hellman 문제의 어려움에 근거하여 *s*를 모르면 g^{Sn}과 g^{Dn}을 악의적이노드가

획득했을 지라도 *K'*를 계산하지 못한다. 따라서 Dn이 키 검증 메세지를 제대로 생성하여 보냈다면, Dn의 *s*를 올바르게 알고 있음을 증명한다.

Sn은 $Sn \in_R [1, q-1]$을 이용하여 g^{Sn}, K, *K'*를 계산한다. 그리고 $H(K \| K')$값을 확인한 후 다음세션을 위해 $H^{n-i}(pwd)$와 *K*를 *MD5*에 적용한 메세지 *H(K)*를 *K'*로 암호화 하여 Dn에게 전송한다. *K'*는 Sn의 다음 세션 *pwd* 검증자를 Dn에게 전송하기 위하여 사용된 인증키이며, Sn과 Dn만이 생성할 수 있는 값이므로 악의적인노드는 *K'*를 생성하지 못하기 때문에 *K'*를 다음세션에 Sn의 *pwd* 검증자를 암호화 하여 보내는데 사용된다. Dn은 Sn로부터 *K'*를 이용하여 복호화 하여 *H(K)*를 확인하고, Sn와 세션키 *K*를 올바로 공유했음을 확인한다. 또한 전송받은 $H^{n-i}(pwd)$에 *MD5*를 적용하여 $H(H^{n-i}(pwd))$과 $H^{n-i+1}(pwd)$이 같은지를 비교한다. 만약 일치한다면 Dn은 Sn과 *pwd*를 올바로 알고 있다는 사실을 인증하게 된다. Sn과 Dn이 적법한 인증절차를 거쳤다면 Dn은 Sn의 $H^{n-i}(pwd)$로 교체하여 디렉토리에 저장한다.

제안 기법에서는 전자서명이 사용된 공개키 요소의 첫 세트를 반복적으로 *MD5*에 적용함으로써 해쉬체인을 생성하고, 해쉬체인으로 부터 공개키 요소들의 여러 세트를 유도한다. 또한 세션키 생성을 통해 안전한 패킷 전송과 데이터를 암호화 할 수 있었으며, 세션키 설정시 *H(pwd)* 암호화 하여 키교환을 수행한다. 검증자는 소스노드와 목적지노드 사이에 *pwd*를 알 수 없으며, *pwd*에서 생성된 검증자를 저장하여 *pwd*가 직접 노출되는 것을 막을 수 있을 뿐만 아니라 악의적인노드의 가장 공격을 막을 수 있는 장점을 가지고 있다.

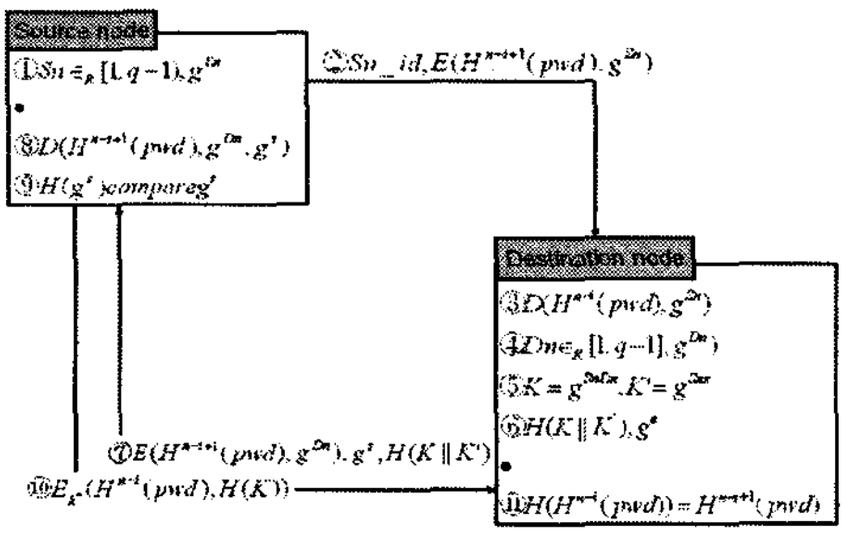

그림 5. 소스노드와 목적지노드 사이의 실행 단계

V. 결 론

본 논문에서는 기존 Ad-hoc 인증기법 및 키 교환 프로토콜의 보안 요구사항을 분석하여 Sn과 Dn사이에 검증자 기반의 OTP를 적용함으로써 Mn간의 강력하고 신뢰성 있는 인증기능을 제공할 수 있었다.

DH-EKE와 OTP S/Key 적용으로 구조가 간단하고 낮은 연산량, 난수 생성횟수, 통신횟수를 줄여 안전하고, 효율성이 강조 되었으면 AODV 라우팅을 함으로써 완전한 Ad-hoc 환경의 상호 인증기법이라 할 수 있다. 또한 기본적인 보안 3요소인 기밀성, 무결성, 가용성에 인증과 부인방지 기능을 추가로 제공하고 있다. Sn과 Dn 사이의 암호화 복호화 과정을 수행함으로써 기밀성을 제공하고, *H()* 특성을 이용하여 Sn과 Dn 사이의 해쉬된 인증을 통해 무결성이 제공된다.

키교환의 수행능력이 높아질수록 가용성은 떨어지지만 이는 암호화와 상반된 관계를 보여 암호화가 높을수록 가용성은 떨어지고 암호화가 낮을수록 가용성은 높아진다. 하지만 가용성을 높이게 되면 악의적인노드의 공격가능성을 더 많이 제공한다고 볼 수 있다. 마지막으로 부인방지로는 Sn과 Dn사이에 해쉬된 검증자를 이용함으로써 Mn간 서명 검증을 수행함으로 부인방지 기능을 제공한다.

참고문헌

[1] Sander van Valkenburg, Asko Vilavaara and Ramjee Prasad, "The Implementation of a Mobile Ad-Hoc Networking Routing Protocol", Proc. of WPM'99, pp.324-330, September, 1999.

[2] Douglas R. Stinson, "Cryptography - Theory and Practice", CRC Press.

[3] T. Wu. The Secure Remote Password Protocol. Internet Society Symposium on Network and Distributed System Security, 1998.

[4] C. Perkins and E. Royer, 'Ad Hoc On-Demand Distance Vector Routing', Ad Hoc Networking, edited by C. E, Perkins, pp.174-201, Addison-Wesley, 2001.