홈 네트워크 내에서의 멀티 홉 통신을 지원하는 인증 프로토콜†

이 주 아, 이 규 환°, 김 재 현

아주대학교 전자공학과

A Novel Authentication Protocol for Multi-hop Communication in Home Network

Ju-a Lee, Kyu-hwan Lee°, Jae-hyun Kim

School of Electrical and Computer Engineering, Ajou University

{gaia, lovejiyoon7, jkim}@ajou.ac.kr

요 약

본 논문에서는 홈 네트워크에서의 멀티 홉 통신 지원을 위한 인증 프로토콜을 제안한다. 홈 네트워크의 특성을 고려하여 멀티 홉 통신을 지원하면서 호스트 인증과 게스트 인증을 할 수 있는 인증 기법을 제안하였다. 본 논문에서는 제안하는 인증 프로토콜이 여러 가지 공격에 강한 면모를 가지고 있는 것을 보이기 위하여 다양한 공격 유형에 대해 방어할 수 있음을 설명하였다. 그리고 제안하는 인증 프로토콜이 홈 네트워크 내에서 데이터 전송 지연에 큰 영향을 미치지 않음을 증명하기 위하여 제안하는 인증 프로토콜을 Linux 시스템에 구현하여 데이터 전송 시간을 측정하였다. 이러한 분석 결과 제안하는 인증 프로토콜은 홈 네트워크의 성능에 큰 영향을 미치지 않으면서도 안전한 홈 네트워크 환경을 제공한다는 것을 보였다.

1. 서 론

홈 네트워크 환경에서 사용될 것으로 예상되는 무선기술은 무선랜과 블루투스, UWB 등이 있다. 이러한 다양한 무선 네트워크의 원활한 통신과 무선 네트워크의 범위가 미치지 않는 음영 지역을 위해서는 애드 혹 네트워크가 지원이 되어야 한다. 애드 혹 네트워크는 별도의 AP(Access Point)나 기반망(infrastructure) 없이 자신이 인식하는 주변 노드들을 연결하여 구성된 망으로 멀티 홉 무선 통신을 제공한다. 애드 혹 네트워크에서는 노드의 이동에 제약이 없고, 네트워크를 동적으로 구성할 수 있는 장점이 있으며 기반망에 기초한 네트워크의 전개가 용이하지 않을 경우 사용될 수 있다. 그러나 동적인 토폴로지 변화, 중앙의 감시와 관리의 결여, 자원의 제약성, 무선 매체의 사용 등의 문제점 때문에 다양한 공격에 노출되기 쉽다. 또한 노드의 신분이 서로에게 불확실한 경우가 많으며 멀티 홉 방식에 의해 라우팅을 할 경우 중간 노드에 의해 발생될 수 있는 데이타 보안 문제도 존재한다. 따라서 애드 혹 네트워크에서는 적합한 사용자임을 증명 받은 노드만이 네트워크 자원을 이용하게 해주는 인증 과정이 중요한 문제이다. 애드 혹 네트워크에서의 인증은 기반망에 기초한 네트워크와 달리 중앙 관리자가 존재하지 않음을 염두에 두어야 한다. 또한 멀티 홉 통신을 위하여 인증 과정이 복잡하지 않고 빠르게 처리될 수 있어야 하며 데이터를 중계해주는 중간 노드의 안전성도 증명되어야 한다. 이를 위해서는 데이터를 전송하기 전에 별도의 인증 과정을 거치는 것보다 라우팅 과정과 동시에 인증 과정을 수행하는 것이 효율적이다. 따라서 본 논문에서는 라우팅 과정에 기초하여 멀티 홉 통신에서의 빠르고 안전하게 인증을 할 수 있는 기법을 제안한다. 또한

† “본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음” (IITA-2006-(C1090-0602-0011))

홈 네트워크는 홈 네트워크의 소유자만 사용하는 것이 아니라 방문자도 사용할 수 있기 때문에 호스트 인증과 더불어 게스트 인증 방식도 제안한다.

관련 연구에는 제 3 의 신뢰된 노드를 이용하는 방법[1],[2]과 클러스터를 이용하는 방식[3] 그리고 라우팅 과정에서 인증과정을 수행하는 ARAN (Authenticated Routing for Ad hoc Networks)[4], SRP (Secure Routing Protocol)[5]등이 있다.

2. 제안하는 인증 프로토콜

2.1 가정 사항

제안하는 인증 프로토콜에서는 사용자가 편리하게 인증 방식을 사용할 수 있도록 기기 인증을 통하여 자동으로 암호화 키를 설정한다. 기기 인증은 사용자가 USB 같은 저장 장치를 기기에 연결하는 형태로 이루어질 수 있으며 근거리 무선 통신을 이용하여 이루어질 수도 있다.

기기 인증은 노드들에게 호스트 키와 인증을 위한 상수 HC_n 을 안전하게 분배하기 위한 과정이다. 여기서 n 은 HC 의 수열을 의미하며 1 부터 m 까지 가능하고, m 은 상수의 최대 사용 개수이다. 노드 i 는 여러 개의 HC_n 중에서 특정 상수 한 개를 선택하여 인증을 수행하도록 하며 이것을 HC_i 라고 한다. 기기 인증 단계를 거친 노드 i 는 다음 연산을 거쳐 홈 네트워크의 소유자의 기기인 호스트를 인증하기 위하여 사용하는 HAK_i (host authentication key)를 얻는다.

$$HAK_i = (K_H, MADDR_i), \tag{1}$$

여기서 K_H 는 호스트 키를 의미하여 $MADDR_i$ 는 노드 i 의 MAC address 를 의미한다. $hash(a,b)$ 는 a 와 b 를 입력 값으로 하는 해쉬 함수의 결과 값이다.

게스트는 홈 네트워크 소유자의 노드가 아니면서 홈 네트워크를 일시적으로 방문하여 접속하기를 원하는 노드를 말한다. 게스트 키 정보는 홈 서버에서 주기적으로 변경시키며 홈 네트워크 내의 호스트 노드들에게 브로드캐스트하여 알려준다. 또는 호스트 인증 과정에서 인증 응답 메시지를 보낼 때 게스트 키에 관한 정보도 포함하여 전송한다. HAK_i 와 마찬가지로 GAK_i (Guest Authentication Key)는 게스트 인증을 위하여 사용되며 다음과 같은 계산으로 얻을 수 있다.

$$GAK_i = (K_G, MADDR_i), \tag{2}$$

여기서, K_G 는 게스트 키를 의미한다.

2.2 호스트 인증 기법

본 절에서는 홈 네트워크 소유자의 노드를 인증하기 위한 호스트 인증 기법을 제안한다. 소스 노드 A, 중간 노드 B, 목적 노드 C 가 있다고 가정할 때 호스트 인증 기법은 다음과 같다.

단계 1: 소스 노드 A 는 라우팅 요청 메시지를 브로드캐스트하며 이 메시지를 전송할 때 다음과 같은 인증 요청 메시지를 함께 전송한다.

$$\begin{aligned} A \rightarrow broadcast : host, ID, \\ \{HC_A, K_A, t_A\}_{HAK_A}, HMAC, \end{aligned} \tag{3}$$

이때 $A \rightarrow broadcast : M$ 은 노드 A 가 메시지 M 을 브로트캐스트 했다는 것을 의미하며 $\{*\}_K$ 는 $*$ 을 키 K 로 암호화 한 것을 의미한다. $host$ 는 노드 A 가 호스트 기기임을 의미하며, ID 는 노드 A 에서 랜덤하게 생성한 메시지 ID 이다. HC_A 는 기기 인증 과정에서 부여 받은 상수 HC_n 중의 하나로 노드 A 가 랜덤하게 선택 한 값이다. HC_A 는 노드들이 동일한 비밀 정보를 공유하고 있는지를 확인하는데 사용한다. K_A 는 노드 A 에서 랜덤하게 생성한 키이다. t_A 는 A 에서의 시스템 시간이며 replay 을 방지하기 위해 사용한다. HC_A, K_A, t_A 는 HAK_A 로 암호화되어 전송되며 $HMAC$ 은 Hashed Message Authentication Code 로 라우팅 메시지를 포함한 전체 메시지의 해쉬값으로 무결성을 확인하기 위해 사용된다.

단계 2: 메시지를 받은 이웃 노드 B 는 라우팅 요청 메시지를 받으면 메시지에 실려있는 노드 A 의 MAC 주소를 얻어내고, 인증 메시지의 종류가 호스트인지 게스트인지를 확인한다. 호스트 인증이라면 기기 인증 때 부여 받은 호스트 키를 이용하여 HAK_A 를 생성한다. 생성된 HAK_A 를 이용하여 메시지를 복호화하여 HC_A 정보를 얻어내고 중간 노드 B 가 기기 인증 때 부여 받은 HC_i 와 비교하여 동일한 값이 존재하는지 찾아본다. 노드 B 는 노드 A 가 적합한 사용자라고 판단을 하면 노드 A 가 보내온 ID, K_A, HC_A 정보와 노드 A 의 MAC 주소 정보를 라우팅 정보와 함께 유지하여 라우팅 응답 메시지를 보낼 때 사용하도록 한다.

단계 3: 중간 노드 B 는 다시 인증 요청 메시지를 생성하여 브로드캐스트한다.

$$A \rightarrow broadcast : host, ID, \{HC_B, K_B, t_B\}_{HAK_B}, HMAC, \quad (4)$$

단계 4: 메시지를 받은 목적 노드 C 는 동일한 방법으로 HAK_B 를 생성하여 메시지를 복호화하고 중간 노드 B 가 보내온 메시지를 인증한다. 목적 노드 C 는 라우팅 알고리즘에 따라 효율적인 경로를 선택하고 라우팅 응답 메시지를 전송한다. 여기서는 A-B-C 경로를 가정한다.

단계 5: 목적 노드 C 는 중간 노드 B 에게 라우팅 응답 메시지를 전송할 때 다음과 같은 인증 응답 메시지를 함께 전송한다.

$$C \rightarrow B : host, ID, \{HC'_C, t_C, L_G, K_G, T_G\}_{K_B}, HMAC, \quad (5)$$

여기서 HC'_C 는 $hash(HC_B, MADDR_C)$ 이고, ID 는 전송 받은 인증 요청 메시지의 ID 이다. 만일 노드 C 가 홈 네트워크 내에서 이미 인증된 노드이고, 홈 서버로부터 게스트 키 정보를 전송 받았다면 노드 C 는 이러한 정보를 인증 응답 메시지를 통하여 다른 노드들에게 알려준다. L_G 는 게스트 키의 길이이며 K_G 는 게스트 키, T_G 는 게스트 키의 유효 시간 정보이다. 이러한 정보는 인증 요청 메시지에 실려있던 노드 B 에서 랜덤하게 생성한 키인 K_B 를 이용하여 암호화되어 전송한다.

단계 6: 인증 응답 메시지를 받은 노드 B 는 K_B 를 이용하여 메시지를 복호화하고 HC'_C 정보가 올바른지 확인한다. 그리고 게스트 키 정보를 받아들이며 A 에게 동일한 방법으로 인증 응답 메시지를 전송한다.

단계 7: 소스 노드 A 는 마찬가지로 HC'_B 정보와 게스트 키 정보를 확인하여 라우팅 과정을 마치고 이후에 전송되는 데이터는 K_A 에 기반한 키를 생성하여 암호화한다.

2.3 게스트 인증 기법

게스트 인증은 홈 네트워크를 일시적으로 사용하기 원하는 노드를 인증하기 위한 인증 기법이다. 소스 노드 A 는 게스트 노드이며 홈 네트워크에 접속하기 위해서는 홈 네트워크 소유자가 직접 게스트 키 정보를 입력해주어야 한다. 중간 노드 B 와 목적 노드 C 는 호스트 노드이며 호스트 인증 과정을 통하여 게스트 키를 알거나 또는 홈 서버로부터 주기적으로 게스트 키 정보를 전송 받는다. 게스트 키를 전송 받은 노드 i 는 GAK_i 를 계산하고, GC 를 생성하여 호스트 인증 과정에서 비밀 정보를 공유하고 있는지를 확인하기 위한 HC_n 을 대신한다. GC 는 게스트 키를 해쉬한 값이다.

단계 1: 소스 노드 A 는 라우팅 요청 메시지를 브로드캐스트하며 이 메시지를 보낼 때 다음과 같은 인증 요청 메시지를 함께 전송한다.

$$A \rightarrow broadcast : guest, ID, \{GC_i, K_A, t_A\}_{GAK_A}, HMAC, \quad (6)$$

여기서 $guest$ 는 인증을 요청하는 노드가 게스트 노드 임을 의미한다.

단계 2: 메시지를 받은 이웃 노드 B 는 라우팅 요청 메시지를 받으면 메시지에 실려있는 노드 A 의 MAC 주소를 얻어내고, 인증 메시지의 종류가 호스트인지 게스트인지를 확인한다. 게스트 인증이라면 GAK_A 생성한다. 생성된 GAK_A 를 이용하여 메시지를 복호화하여 GC 정보를 얻어내고 B 가 계산한 GC 와 동일한지를 비교한다. 중간 노드 B 는 소스 노드 A 가 적합한 사용자라고 판단을 하면 노드 A 가 전송한 ID , K_A 및 노드 A 의 MAC 주소 정보를 유지하여 라우팅 응답 메시지를 보낼 때 사용하도록 한다.

단계 3: 중간 노드 B 는 동일한 방법으로 인증 요청 메시지를 생성하여 브로드캐스트한다.

단계 4: 메시지를 받은 목적 노드 C 는 메시지를 복호화하고 B 가 보내온 메시지를 인증한다. 목적 노드 C 는 라우팅 알고리즘에 따라 효율적인 경로를 선택하고 라우팅 응답 메시지를 전송한다. 여기서는 A-B-C 경로를 가정한다.

단계 5: 노드 C 는 노드 B 에게 라우팅 응답 메시지를 전송할 때 다음과 같은 인증 응답 메시지를 함께 전송한다.

$$C \rightarrow B : guest, ID, (GC'_C, t_C)_{K_B}, HMAC, \quad (7)$$

여기서 GC'_C 는 $hash(K_G, MADDR_C)$ 이고, ID 는 전송 받은 인증 요청 메시지의 ID 이다.

단계 6: 인증 응답 메시지를 받은 노드 B 는 K_B 를 이용하여 메시지를 복호화하고 GC'_C 정보가 올바른지 확인한다. 그리고 노드 A 에게 동일한 방법으로 인증 응답 메시지를 전송한다.

단계 7: 소스 노드 A 는 마찬가지로 GC'_B 정보를 확인하여 라우팅과정을 마치고 이후에 전송되는 데이터는 K_A 를 이용하여 암호화한다.

3. 성능 평가

3.1 Security 분석

본 절에서는 다양한 공격 유형들을 고려하고, 제안한 인증 프로토콜이 이러한 공격들을 어떻게 방어할 수 있는지에 대하여 서술하고 제안한 프로토콜의 안전성을 평가한다.

도청: 도청은 무선으로 전송되는 데이터의 내용을 공격자가 가로채어 살펴보는 것을 의미한다. 그러나 제안하는 프로토콜에서 인증 메시지는 암호화되기 때문에 공격자가 메시지를 도청할 수 없다.

Replay 공격: replay 공격은 노드 간에 이미 전송된 메시지를 가로채어 수집하여 두었다가 공격자가 이를 그대로 사용하는 공격 유형이다. 제안한 프로토콜에서는 인증 메시지에 메시지를 전송하는 노드의 MAC 주소 정보가 포함되어 있다. 따라서 메시지 내의 MAC 주소와 메시지를 전송하는 노드의 MAC 주소가 동일하지 않으면 수신 노드는 인증 메시지가 공격 메시지라는 것을 알 수 있다. 또한 타임스탬프 값을 이용하여 제한된 시간 내에만 인증 메시지가 유효하도록 하여 replay 공격을 방지한다.

패스워드 추측 공격: 패스워드 추측 공격은 공격자가 추측한 패스워드를 이용하여 메시지를 복호화하는 방법이다. 그러나 제안한 프로토콜에서 암호화되는 부분 중에 고정된 값은 존재하지 않는다. 예를 들어, 호스트 인증 요청 메시지를 보면 HC_n 의 개수는 한정 되어 있기는 하지만 노드가 메시지를 전송할 때마다 계속 변화된다. 또한 K 값은 랜덤한 값이며, 정확한 타임스탬프 값을 공격자가 알아내기 어렵다. 게스트 키도 주기적으로 변경되는 값이며 노드마다 암호화하는 키가 다르기 때문에 여러 개의 노드들이 보낸 메시지를 동시에 복호화하여 같은 HC_i 또는 GC 값을 찾아내기 어렵다.

메시지 변조: 공격자가 임의로 메시지의 일부분을 수정하는 공격 유형을 생각해볼 수 있다. 그러나 제안하는 프로토콜에서는 을 사용하기 때문에 메시지의 일부분에 수정이 가해지는 것을 알아낼 수 있다. 만일 공격자가 메시지의 일부만 수정하면 값이 전혀 달라지기 때문이다

3.2 전송 지연 시간 분석

제안한 애드 혹 인증 알고리즘의 성능 분석을 위하여 본 절에서는 데이터 전송 지연 시간을 분석한다. 제안하는 알고리즘을 리눅스에서 구현을 하여 실제 데이터를 전송하여 전송 시간을 측정 하였다. 기본 개발 환경은 표 1 과 같다. 구현을 위하여 사용된 키 값은 16byte 이며 인증을 위한 상수 HC_n 은 2byte 씩 총 5 개를 사용하였고, AES (Advanced Encryption Standard) 암호화 알고리즘 방식과 MD5 해쉬 알고리즘을 사용하였다.

제안하는 인증 프로토콜이 데이터 전송 지연에 미치는 영향을 측정하기 위해 제안하는 인증 프로토콜을 구현한 애드 혹 네트워크와 구현하지 않은 애드 혹 네트워크에서의 데이터 전송 지연 시간 차이를 비교하였다. 인증 시간은 데이터 크기와 무관하게 고정되어 있기 때문에 ping 을 통하여 전송 시간을 측정 하였으며 1 홉과 2 홉에서 각각 총 100 회를 측정하였다. 1 홉 실험에서는 노드 A 와 노드 C 를 15m 떨어뜨리고 실험을 하였으며 2 홉에서의 성능을 측정하기 위하여 노드 A 와 노드 B, 노드 C 를 각각 15m 떨어뜨리고 노드 A 에서 노드 C 로 ping 메시지를 전송하였다. 실험 결과는 그림 1 및 그림 2 와 같으며 그림에서 보듯이 제안하는 인증 프로토콜이 데이터 전송 지연에 큰 영향을 미치지 않음을 알 수 있다. 1 홉에서 인증 프로토콜을 사용하지 않을 때의 평균 전송 시간은 4.94ms 이며 인증 프로토콜을 사용할 경우는 평균 5.04ms 로 100 μs의 차이를 보였다. 이러한 결과는 무선 환경에서의 감쇄, 지연 현상 등을 감안하면 인증 프로토콜을 사용한다고 하더라도 실제 데이터 전송 시간에 미미한 영향만이 있다는 것을 알 수 있다. 2 홉에서는 인증 프로토콜을 사용하지 않을 경우의 평균 전송 지연 시간은 10.57ms 이며 인증 프로토콜을 사용할 경우는 11.28ms 로 710 μs의 차이를 보였다.

표 1. 기본 개발 환경

항목	개발 환경	버전	비고
operating system	Linux Fedora Core 5	커널 2.6.15	
무선 기기	Ralink Tech RT2571w 모델 무선 랜 카드 802.11b/g 지원	1.0.3.6	노드 A
	Intel Pentium 4, 280 GHz CPU, 1 GB RAM		
	Ralink Tech RT2571w 모델 무선 랜 카드 802.11b/g 지원	1.0.3.6	노드 B
	Intel Celeron M, 1.5 GHz CPU, 256 MB RAM		
	Intel ipw2200 모델 무선 랜 카드 802.11b/g 지원	1.1.3	노드 C
	Intel Petium M 745, 1.8 GHz CPU, 1 GB RAM		

제안하는 인증 프로토콜을 사용함으로써 지연되는 이론적인 시간을 구해보면 약 2.7 ㎲의 시간이 소요된다. 이 경우는 RAM 1GByte 와 AMD 1.6GHz 의 프로세서를 사용할 경우 1 홉에서 지연되는 시간이다.

제안하는 인증 알고리즘은 빠른 인증을 수행하기 위하여 인증서 방식이나 공개키 방식이 아닌 패스워드 방식을 사용하였다. 따라서 결과에서 보는 바와 같이 제안하는 인증 프로토콜이 데이터 전송 지연에 큰 영향을 미치지 않으면서도 네트워크 보안을 강화하며 공격자로부터 안전한 데이터 전송을 보장할 수 있다.

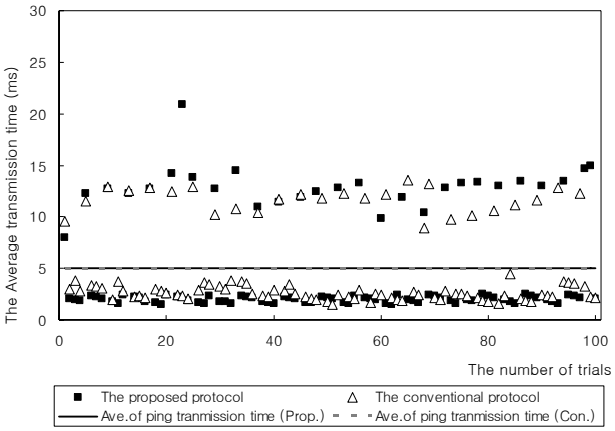

그림 1. 1 홉에서의 ping 전송 지연 시간 비교

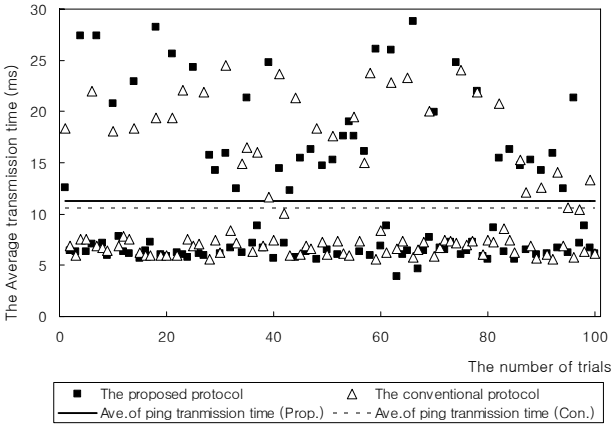

그림 2. 2 홉에서의 ping 전송 지연 시간 비교

4. 결 론

본 논문에서는 홈 네트워크 내의 애드 혹 네트워크를 위하여 멀티 홉 통신을 지원하는 인증 프로토콜을 제안하였다. 그리고 홈 네트워크 환경을 고려하여 호스트 인증과 게스트 인증을 구별하였기 때문에 보다 안전한 인증을 수행할 수 있다. 제안하는 인증 프로토콜은 인증서 방식이나 공개키 방식을 사용하지 않기 때문에 가볍고 빠른 인증을 수행할 수 있으며 상호 인증과 메시지 암호화에 서로 다른 키를 사용하여 공격에 대한 안전성[6]을 높였다. 세션 키의 seed 값으로 사용될 수 있는 키 K는 인증 과정에서 생성하여 홉 마다 다른 암호화 키로 암호화되어 전달 되기 때문에 안전하며 K를 생성한 노드는 자신이 전달하였던 비밀 정보와 상대 노드의 정보를 K를 이용하여 암호화되어 전달받기 때문에 세션 키의 seed 값이 올바르게 전달이 되었는지 확인할 수 있다. 또한 중간 노드에 대한 인증을 수행하여 멀티 홉 통신을 지원할 뿐만 아니라 홉 수가 늘어날수록 전달되는 메시지의 양이 증가하지도 않는다.

본 논문에서는 다양한 공격 유형에 대하여 제안한 인증 프로토콜이 어떠한 강점을 갖는지 분석하였으며, 분석 결과로 제안한 프로토콜은 홈 네트워크 내의 애드 혹 네트워크에서 안전하고 효율적인 인증 프로토콜로 사용될 수 있다.

5. 참고 문헌

[1] A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", in Proc. ACSC'04, pp. 41-46, Dunedin, New Zealand, Jan. 18-22, 2004.

[2] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and Identity-based Key Management and. Authentication for Wireless Ad Hoc Networks", in Proc. ITCC’04, vol. 1, pp. 107-111, Las Vegas, U.S.A., Apr. 5-7, 2004.

[3] M. Bechler, H.-J. Hof, D. Kraft, F. Phlke, and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", in Proc. INFOCOM 2004, vol. 4, pp. 2393-2403, Hong Kong, Mar. 12-13, 2004.

[4] K. Sanzgiri, D. Laflamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks", in Proc. IEEE Journal on Selected Areas in Communications, Vol. 23, no. 3, Mar. 2005, pp. 598-610.

[5] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", in Proc. CNDS 2002, pp. 193-204, San Antonio, TX, Jan. 27-31, 2002.

[6] H. X. Mel and D. Baker, Cryptography Decrypted, Addison-Wesley, 2000.