제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

이동 Ad-hoc 망에서 보안 지원 기술

성연주, 김민정, 김기천
*건국대학교 컴퓨터공학과
e-mail : mejuma@cse.konkuk.ac.kr

A Study on Security for Mobile Ad-Hoc Protocol

Youn-Ju Seong, Min-Jeong Kim, Kee-Cheon Kim
Dept. of Computer Engineering, Kon-Kuk University

요 약

최근 무선 환경에서의 이동 노드들간의 라우팅을 지원하는 이동 Ad-Hoc 네트워크에 대한 연구가 활발히 이루어지고 있다. 이동 Ad-hoc 네트워크는 기반 시설이 존재하지 않거나 설치가 용이하지 않은 지역에서 고정된 기반망의 도움없이 이동 노드들간에 자율적으로 구성되는 망이다. 본 논문에서는 이동 Ad-Hoc 네트워크의 기술현황을 살펴보고 현재 논의되고 있는 주요 기술 이슈에 대해 알아보았다. 특히 Ad-Hoc 네트워크는 무선의 특성상 보안에 취약하므로, 보안성을 지원하기 위한 기술들을 중점으로 살펴보았다. Ad-Hoc 네트워크의 보안 기술로는 ARAN, SAR, Ariadne , SEAD 등 이 있다.

1. 서론

이동 Ad Hoc 네트워크는 고정된 기반 망의 도움없이 이동 노드들간에 자율적으로 구성되는 망으로서, 네트워크에 자율성과 융통성을 부여한 네트워크이다 [1]. Ad-hoc 망은 모든 단말기가 이동하는 환경에서 서로 직접적인 무선 전송 범위에 위치하지 않은 노드간의 원활한 데이터 전송을 위해 다중 홉 무선링크로 구성되어 여러 개의 중간 단말기들의 데이터 포워딩/경로설정(Forwarding/Routing)에 의존하게 되는 새로운 형태의 통신망이다. 따라서 신속하게 통신망을 구성할 수 있고 기존 통신 인프라에 의존하지 않으며 단말기 이동에 빨리 적응을 할 수 있는 장점을 가진 통신망이라 할 수 있다. Ad-hoc 통신망은 기존 인프라가 필요치 않는 특성으로 인하여 임시 구성용 네트워크이나 지진, 태풍, 테러에 의한 재해/재난지역과, 특히 전쟁터와 같은 기반 시설이 없는 환경에서 적용가능토록 주로 군사용 망에 중점을 두어 연구 개발되어 왔다.

그러나, Ad Hoc 네트워크는 무선의 고유특성으로 인해 여러 가지 보안상 위협에 취약한 면을 지니고 있다. 이러한 위협들의 예로는 무선채널을 통한 엿듣기, 트래픽 모니터링과 같은 수동적인 공격과 악의적인 사용자로부터의 서비스 거부 공격(Denial Of Service), 그리고 신뢰성이 손상된 개체나 도난 당한 장치로부터의 공격등과 같은 능동적인 공격이 있다. 임의의 네트워크 환경에서 이러한 공격에 대한 안전한 통신을 보장하기 위해서 기밀성, 인증, 무결성 그리고 가용성 등을 충족시켜야 한다. 이러한 보안상의 요구는 적절한 키 관리 방법을 필요로 한다. 하지만 기존의 방법들은 키의 일치를 위해 과도한 통신 오버헤드, 오랜 지연시간을 요구하거나 안전상 취약점을 노출한다. 본 논문에서는 Ad Hoc 기술 현황에 대해 살펴보고, 위와 같은 특징을 지닌 Ad Hoc 네트워크에서 안전한 데이터 전송을 위한 인증, 보안 프로토콜에 대한 기술동향을 살펴본다.

2. 이동 Ad-hoc 망 기술현황 및 주요 기술 이슈

무선 Ad-hoc 망 구성기술과 관련된 국외의 동향을

살펴보면, 우선 인터넷 표준 제정을 위한 국제기구인 IETF(Internet Engineering Task Force)의 경우 MANET 이라는 작업그룹이 결성되어 다수의 RFC 와 인터넷 드래프트(Internet draft)가 나와 있다. IETF MANET 의 목표는 무선 Ad-hoc 망에서의 인터넷 프로토콜 지원 및 효과적인 라우팅 지원 방안의 표준화이며, 현재까지의 제안된 연구내용은 라우팅과 관련된 것이 대부분이다 [2].

미국의 DARPA 에서 지원하고 있는 GloMo 프로그램의 경우, 군용 무선 Ad-hoc 망 구축을 위한 애플리케이션, 라우팅, MAC, SDR(Software Defined Radio) 모뎀 및 안테나 등에 관한 연구를 통하여 군용 무선 Ad-hoc 망 구성 요소들의 프로토타입 개발을 수행하고 있다. 이는 ACN 등의 무인비행기를 활용한 인프라에 Ad-hoc 기술을 적용하는 영역까지 확대되고 있다. GloMo 프로그램에는 CMU, MIT, Rutgers, Stanford, UC Berkeley, UCLA, Kansas, Virginia Tech 등의 유수한 미국내 대학들과 Raytheon Systems Company, Rockwell International 등의 기업들이 참여하였으며 현재 프로젝트는 완료된 상태이다. Lucent Bell Labs 와 Sun Microsystems 의 광대역 Ad-hoc 무선 ATM 근거리 통신망을 위한 BAHAMA 프로젝트 역시 현재 연구 중인 무선 Ad-hoc 망의 다른 예이다. 이외에도 CMU 의 Monarch(Mobile Networking Architecture) 프로젝트와 같은 무선 Ad-hoc 망과 관련된 프로젝트들이 대학을 중심으로 활발히 진행 중에 있다.

최근에는 군용, 재난 지역의 임시 망 이외에 구내 통신망에 무선 Ad-hoc 망을 적용하기 위한 기술 개발과 연구가 활발하게 진행되고 있다. 일반 가정의 PC 및 주변기기, 전화와 휴대폰 등의 통신기기 및 가전제품 등을 단일 프로토콜로 제어하기 위한 개념에서 출발한 홈 무선 통신망(wireless home networking) 기술은 미래의 정보 통신 분야를 선도할 첨단 기술로 인식되고 있다. 이에 따라 Microsoft, IBM, Intel, Nokia, Ericsson, HP, AT&T, Cisco 등 통신/정보 장비, 서비스, 통신 업체 등이 연구그룹을 결성해 사설 무선 근거리 통신망 기술 개발에 적극적으로 참여하고 있다.

국내에서는 대학 및 연구소에서 Ad-hoc 망의 MAC 계층과 라우팅 기술에 대하여 기초적인 연구를 부분적으로 진행하여 왔으며 최근 들어 차세대 이동통신 및 WAN, PAN 의 연구와 맞물려 많은 관심을 가지고 활발하게 연구를 시작하려는 단계이다. 그러나 현재까지 이동성이 지원되는 Ad-hoc 망에 대한 전반적인 성능 분석, 기술 제안과 구현 등의 사례가 극히 부족하며 본격적인 연구가 절실한 편이다.

선진국에서는 이동성을 지원하는 Ad-hoc 망에 대한 기술 확보가 국가적인 차원에서 연구개발 및 구현이 매우 활발히 되고 있으며 전통적인 군수산업 및 군사 연구소에서의 연구 활동에 덧붙여 최근 셀룰러 이동통신의 대체 또는 보완을 목적으로 상용화를 시도하는 벤처기업까지 등장, 현재 실용화 추진을 위하여 노력하고 있다. 그에 비하여 국내에서는 기초적인 연구 부분에서만 일부에서 실시하고 있으므로 국가 차원에서의 Ad-hoc 망에 대한 연구 개발과 구현이 필요하다. 현재 이동성이 지원되는 Ad-hoc 망에 대한 라우팅과 자원의 이동 관리와 같은 분야들은 소규모 그룹을 위한 네트워킹에서 구체적으로 적용을 위한 세부설계가 필요하며, Ad-hoc 전반에 걸쳐서도 아직 실제로 구현되지는 않은 단계이다. 기존의 Ad-hoc 망은 이동성이 커질수록 프로토콜의 성능저하도 커지므로 보다 효율적인 프로토콜을 연구해야 할 것이다.

현재 주로 논의되고 있는 Ad-hoc 망에 대한 이슈로는 기존의 Ad-hoc 라우팅 프로토콜에 효율적인 이동성을 제공하는 보완작업, 보안성과 데이터 무결성을 지원하기 위한 방안, Energy Efficiency 라우팅 정보 관리 기법, Ad-hoc 망의 이동성을 지원하기 위한 호스트와 망 차원의 이동 관리기술, 이동 Ad-hoc 망과 다른 망과의 상호 운용성 지원하기 위한 방안들이 연구되고 있다. 그중에서 이동 Ad-Hoc 네트워크에서 보안성을 지원하기 위한 프로토콜에 관하여 자세히 알아본다.

3. 이동 Ad-Hoc 보안 프로토콜

Ad-hoc 망은 기존의 유선 네트워크와는 달리 네트워크 내의 모든 단말에 기본적으로 데이터를 전송하는 브로드캐스팅 방식을 사용하므로 모든 단말은 다른 사람의 송수신 데이터 내용을 청취할 수 있어서 의도된 수신자 이외의 다른 사람으로부터 데이터를 보호하기 위해서는 기밀성 및 무결성, 상호 인증에 관한 서비스가 중요하다. 이동 Ad-Hoc 네트워크에서 야기되는 보안관련 문제로는 인접한 노드가 잘못된 라우팅 업데이트 정보를 광고하는 노드의 신뢰성 문제, 노드의 과부하와 깨짐 등에 대한 이유로 생긴 불량노드에 의한 처리량 증가, 프로토콜 필드의 변화에 따르는 메세지 공격, 원거리 공격에 의한 redirection 등이 있을 수 있다.

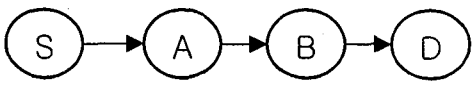
매체를 신뢰할 수 없는 Ad-hoc 망의 특성상 암호를 사용할 수 없기 때문에 암호 키 방식에 크게 의존하게 된다. 따라서 키 사이에 신뢰할 수 있는 관계를 형성하고 이를 Ad-hoc 망 전반에 분배하는 것이 주요 보안 이슈라고 할 수 있다.

이동 Ad-Hoc 망에 보안성을 지원하기 위한 프로토콜로는 ARAN, SAR, Ariadne , SEAD 등 이 있다.

ARAN(Authenticated routing for ad hoc etwork)

ARAN 은 On-Demand Ad-Hoc 라우팅 프로토콜 방식에서 이동 노드의 인증, 데이터 무결성을 지원하기 위해 사용된다. ARAN 은 인증서버가 필요한 공개키 기반 구조를 이용한다. 때문에 경로 요청/응답 과정에서 모든 단말들이 라우팅 관련 작업을 수행하고 패킷을 전송할 때마다 자신의 인증서를 부가적으로 붙여야 하므로 데이터의 길이가 늘어나 이동 노드에 부담을 주게 된다. ARAN 은 end-to-end authentication 구조를 가지며, source 노드는 오로지 return path 에 의해 선택된 노드에 대해서만 신뢰한다. 이것은 경로상의 모든 단말들을 인증할 수 없다는 단점을 지니게 된다.

새로운 네트워크에 들어가기 전에 Ad-Hoc 노드들은 인증을 받기 위해 신뢰할 수 있는 서버로부터 Public key 를 받아야 한다. Route Discovery 시 source 노드는 자신의 IP address, 인증서, 중복을 방지하기 위한 source specific nonce 를 포함한 RDP(Routing Discovery Packet)를 보낸다. RDP 를 받은 노드는 자신의 signature 와 인증을 추가하여 다음 노드로 전송한다. 서명을 추가함으로써 loop 나 경로변경 등의 공격을 방지할 수 있게 된다. 목적지 노드는 RDP 메시지와 nonce 값에 응답하여 REP 메시지를 보낸다. REP 를 처리하는 중간 노드 역시 이전 노드의 서명을 검증하고 자신의 서명으로 다시 인증하여 전송한다[4][5].



S-> broadcast : [RDP, IP_D, $Cert_S$, N_S, t]K_S.
A-> broadcast : [[RDP, IP_D, $Cert_S$, N_S, t]$K_{S.}$]$K_{A.}$, $Cert_A$
B-> boradcast : [[RDP, IP_D, $Cert_S$, N_S, t]$K_{S.}$]$K_{A.}$,$Cert_B$

SAR (Security-Aware Ad-Hoc Routing for Wireless Network)

기존의 Ad-Hoc 라우팅 프로토콜은 경로선택 시 보안에 대한 고려 없이 홉수를 기준으로 사용해왔다. SAR 에서는 일반적인 라우팅 메트릭 요소로 노드의 보안 레벨을 포함한다. SAR 은 On-demand 라우팅 방식인 AODV 의 기본 동작절차를 바탕으로 하여 경로 탐색을 요청하는 RREQ 와 그에 대한 응답인 RREP 패킷 내에 보안 메트릭 값을 내장하는 방식을 사용한다. RREQ 내의 RQ_SEC_REQUIREMENT 필드에는 경로에서 요구하는 보안 레벨을 포함하며, 요구된 보안 레벨보다 낮을 경우에 RREQ 패킷은 폐기되므로, 목적지에 RREQ 가 도착하면, 목적지까지의 경로의 보안 레벨은 RQ_SEC_REQUIREMENT 필드내의 보안 레벨을 만족하는 경로, 즉 Secure Route 임을 의미한다.

SAR 은 이동 Ad-Hoc 환경에서 안전한 경로를 발견할 수 있게 하며, DSR 이나 AODV 와 같은 기존의 On-demand 라우팅 프로토콜에 쉽게 적용할 수 있다. SAR 을 적용함으로서 발생하는 오버헤드는 RREQ/RREP 메시지의 플러딩 범위를 제한함으로서 감소시킬 수 있다.

Ariadne(A Secure On-Demand Routing Protocol for Ad-hoc Networks)

또 다른 프로토콜로 Ariadne 이 제안되었는데 Ariadne 은 On-Demand 방식의 프로토콜인 DSR 을 기반으로 하며 대칭키를 사용하는 보안관련 프로토콜이다. Ariadne 프로토콜은 네트워크 계층 이하는 고려하지 않으며 양방향 통신을 가정한다. Ariadne 에서 사용되는 키 설정 메커니즘은 Pair-wise shared 비밀키와 디지털 서명, TESLA 이다.

TELSA(Timed Efficient Stream Loss-tolerant Authentication)는 브로트 캐스팅이나 멀티캐스팅 통신에서 계산적 과부화가 적은 해쉬 함수를 사용하고 시간 지연적 키 노출방법을 사용하여 각 패킷의 인증을 수행하는 방식으로 송신자는 인증키를 키 노출시간이 지난 후에 전송 패킷에 실어 보내주며 수신자는 그 노출 시간이 지난 후에 이전에 받은 패킷을 인증할 수 있다. 인증키는 one-way key chain 을 사용하여 시간의 역방향으로 계산되므로 중간에서 임의로 생성할 수 없으며 패킷의 손실에 강하다는 장점이 있다. TESLA 는 시간 지연적 키 노출 방법을 사용하므로 송신자와 수신자간에 시간 동기화(time synch)가 필요하다.

Ariadne 는 목적지 노드가 협의되지 않은 이웃에 관한 정보를 가지고 있을 때 route reply 를 리턴한다. 출발지에 하나의 route reply 라도 반환된다면 Ariadne 는 route reply 내의 정보를 바탕으로 협의되지 않은 경로를 따라서 패킷을 전송할 수 있다. attack 을 방지하기 위해 hop 단위로 해싱한 인증코드를 사용하며 TESLA 의 최대 종단 지연 특성과 hash chain 을 사용한다.

Ariadne 는 모든 중간 단말들에 대한 인증이 가능하단 장점을 지니고 있으나, 미리 각 단말간의 시간동기화 및 최대 전송 지연시간을 알아야만 한다. 자신을 제외한 모든 단말들에 대한 해쉬 사슬값을 공유, 갱신해야 하므로 중간 단말의 MAC 값을 패킷에 추가해야 해야만 하는데 이것은 패킷으리 길이를 길어지게 하므로 네트워크와 노드의 자원을 많이 소비하게 하는 단점을 지니고 있다.

SEAD(Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks)

SEAD 는 Table-driven 라우팅 프로토콜인 DSDV 을 기반으로 단 방향 Hash Chain 을 사용하여 인증과 데이터 무결성을 제공하는 프로토콜이다. DSDV 프로토콜은 구현이 용이하고, 제한된 메모리와 CPU 같은 제한된 자원 활용의 측면에서 효율적인 장점이 있다. 단 방향 Hash Chain 은 단 방향 hash 함수를 사용하여

계산이 단순하고, 입력 값에 매우 종속적이기 때문에 입력 값의 비트가 하나만 바뀌어도 전혀 다른 해쉬값이 나오기 때문에 어떤 결과 값이 나올지 전혀 예측할 수 없다. 이런 예측 불가능 성 때문에 주어진 해시 결과 값으로부터 원래의 입력을 거꾸로 계산할 수 없으므로 메시지 암호화에 많이 사용된다.

SEAD 를 적용하는 네트워크 내의 모든 무선링크는 양방향임을 가정하며, 패킷의 손실이나 복사, 전송 순서의 변경이 발생할 수 있는 가능성을 가정한다. SEAD 는 DSDV 를 기반으로 하기 때문에 목적지 시퀀스 번호를 사용하여 라우팅 루프의 발생을 막고 라우팅 업데이트 메시지의 Replay attack 을 방지한다.

4. 결론

최근 이동 Ad-hoc 네트워크에 대한 활발한 연구가 진행되고 있다. Ad-hoc 네트워크는 인터넷과 같은 기반 네트워크에 완전히 독립된 형태로 존재하거나 또는 이에 연동되는 형태로 존재할 수 있다. 이러한 Ad-Hoc 네트워크의 특징은 이동 Ad-hoc 망은 비행기, 철도 또는 대형 선박 등 많은 단말기가 집단을 이루어 동시에 이동하는 경우나, 재난이나 군사작전 등과 같이 단말기의 이동성을 지원하면서 빠르게 네트워크를 구성할 필요가 있을 때 매우 유용하다. 그러나, Ad Hoc 네트워크는 무선의 고유특성으로 인해 여러 가지 보안상 위협에 취약한 면을 지니고 있다. 때문에 안전한 통신을 보장하기 위해서 기밀성, 인증, 무결성 그리고 가용성등을 충족시켜야 한다.

본 논문에서는 Ad-Hoc 네트워크에 보안성을 지원하기 위한 프로토콜로 ARAN, SAR, Ariadne , SEAD 등에 대해 알아보았다. 이 외에도 많은 프로토콜들이 연구되고 있으며 앞으로 Ad-hoc 네트워크의 특성상 노드의 부하를 줄이면서 강력한 라우팅을 지원하는 방향으로 연구가 이루어질 것이다.

참고문헌

[1] C.E. Perkins, Ad-hoc Networking, Addison-Wesley, 2001.

[2] 이동 Ad-hoc 네트워크 기술동향, 권혜연 외 5 인, 전자통신 동향분석 18 권 제 2 호, 2003

[3] Ad-hoc 통신망 프로토콜 개발동향, 김종천, Telecommunication review 제 12 권 3 호, 2002

[4] Authenticated Routing for Ad hoc network, Elizabeth M. Beloding-Royer

[5] http://signl.cs.umass.edu/arand

[6] Power-Saving Protocols for IEEE 802.11-Based Multi-Hop Ad Hoc Networks, Yu-Chee Tseng, Chih-Shun Hsu, Ten-Yueng Hsieh