제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

Ad-Hoc 라우팅 프로토콜에서의 보안

김민정, 김기천
e-mail : saojeong@konkuk.ac.kr

Secure Routing Protocol in Ad-Hoc Network

Minjeong Kim, Keecheon Kim
Dept. of Computer Science& Engineering, Kon-Kuk University

요 약

Ad-Hoc 네트워크는 네트워크 내의 노드들이 이동 노드로서의 역할 뿐 아니라 라우터로서의 역할도 담당하여 기존의 인프라를 통한 중앙관리 및 지원 없이 네트워크 내의 무선 이동 노드들만으로 망을 구성하며, 네트워크의 특성상 보안이 취약하다는 단점이 있다. 현재 Ad-Hoc 네트워크는 그 적용 범위와 활용 빈도가 확대되고 있으며, 네트워크 분야에서의 비중이 증가하고 있으므로 유선에서 제공하는 수준의 보안을 제공할 수 있도록 해야 한다. 그러나 관련연구는 아직 취약한 실정이므로 현재 표준으로 제안된 라우팅 프로토콜을 기반으로 보안을 제공하기 위해 제안된 프로토콜에 관해 살펴본다.

1. 서 론

최근 무선 네트워킹 분야의 급속한 기술 발달로 이동 무선 네트워크에 대한 요구사항이 점점 증가하고 있는 추세이다. 원래 군사적인 목적을 위해 개발된 Ad-Hoc 네트워크는 이제 군용망 뿐 아니라 상용망에서도 그 적용 범위와 빈도가 확대되고 있다.

Ad-Hoc 네트워크란 기존 유선 네트워크의 통신 인프라의 지원 없이 단말기 간의 라우팅 만으로 데이터의 송수신을 수행하는 무선 네트워크를 뜻한다. 자연재해, 전시 상황과 같이 기반 시설이 없는 환경이나 기지국, AP 등의 고장으로 인해 유선 네트워크와의 단절이 발생한 경우에도 단말기 자신이 단말로서의 기능 뿐 아니라 라우터, 서버의 역할을 수행하여 단말기 각각의 동적인 상태 및 위상 변화를 실시간으로 반영하여 통신을 지원할 수 있다.[1]

그러나 Ad-Hoc 네트워크는 전달매체로 물리적인 매체가 아닌 대기를 이용하며, 기본적으로 네트워크 내의 모든 단말에 데이터를 전송하는 브로드캐스팅 방식을 사용하므로 모든 단말은 다른 사람의 송수신 데이터 내용을 쉽게 청취할 수 있어 의도된 수신자 이외의 다른 사람이 데이터를 도청하거나, 이를 이용한 악의적인 공격을 당할 가능성이 크다.

무선 네트워크의 기반 기술로서의 Ad -Hoc 네트워크의 중요성이 점점 증대됨과 동시에 보안의 중요성 역시 커지고 있다.

본 논문에서는 보안에 취약한 Ad-Hoc 네트워크에서 보안을 지원하기 위해 고려해야 할 사항 및 이를 바탕으로 제안된 몇몇 보안 라우팅 프로토콜에 관해 살펴보고자 한다.

2. Ad-Hoc 네트워크의 특징

Ad-Hoc 네트워크는 중앙의 통제로부터 완전히 독립하여 사용자로 하여금 네트워크 사용 시 더 많은 자유와 유연성을 확보할 수 있도록 하며, 네트워크 구성과 이동이 용이하다는 특징을 가지고 있다.

Ad-Hoc 네트워크의 특징은 크게 다음과 같다.

가. 분산 네트워크 : Ad-Hoc 네트워크 상의 노드들은 기존 인프라의 지원 없이 보안 및 라우팅 기능을 수행하여야 하며, 중앙관리를 담당하는 노드가 없기 때문에 각각의 기능을 네트워크 내의 노드에 분산시켜 수행하도록 한다.

나. 동적 위상 : Ad-Hoc 네트워크는 네트워크의 위상이 빈번하게 변경되므로 노드의 상태를 반영하는 다양한 네트워크 형태를 구성할 수 있으며, 네트워크의 위상 변화에 관계없이 지속적으로 서비스를 제공할 수 있어야 한다.

다. 제한된 자원 : 네트워크 내의 노드들은 CPU 와 메모리, 배터리와 같은 자원의 사용이 제한되어 있으므로, 불필요한 자원낭비가 발생하지 않도록 효율적

인 알고리즘과 메커니즘을 적용하여 최소한의 자원사용으로 최대한의 처리가 가능하도록 해야 한다.
라. 무선 취약성과 제한된 물리적 보안 : Ad-Hoc 네트워크는 일반적으로 고정망보다 정보와 물리적 보안 위협에 더 많이 노출되어 있으나 이를 보완하기 위한 관련 연구는 아직 미흡한 실정이다.

3. 개발동향

3.1 Manet (Mobile Ad Hoc Networks) WG

Manet 워킹그룹은 Mobile Ad-hoc 환경에서 이동 단말들 간의 통신에 필요한 라우팅 프로토콜을 연구하고 개발 하는 IETF 산하의 표준화 단체로서 유니캐스트 라우팅 프로토콜의 표준인 AODV, DSR 등을 비롯하여 멀티캐스트 라우팅 프로토콜 및 Flooding, MAC, Multi-channel Mac, 저전력 소비 등에 관한 연구를 수행하고 있다.

현재 Manet 에서 표준 유니캐스트 라우팅 프로토콜로 제안된 RFC 인 AODV[2]를 비롯하여 소스 라우팅 방식에 기반한 DSR (Dynamic Source Routing)[3], OLSR (Optimized Link State Routing)[4], TBRPF (Topology Broadcast Based on Reverse-Path Forwarding)[5] 등이 Internet Draft 로 제안되 있으며, 수정 및 보완 활동이 활발하게 진행되고 있다.

3.2 Glomo(Global Mobile Information System) Project

이동 Ad hoc 망 연구는 1973 년부터 시작된 미국 DARPA(Defense Advanced Research Projgects Agency)의 PRnet(Packet Radio Network)에서 군사 목적의 통신 시스템 개발을 위해 처음 시작되었다. DARPA GloMo(Global Mobile Information System) 프로젝트는 사용자 친화적 연결성과 무선 이동 사용자를 위한 서비스로의 접속 기능을 제공하여 방위 정보 기반 구조에서 이동 환경을 최우선적으로 고려하며, 다중 홉의 독자적인 구성이 가능하고 수직적 핸드오프를 수행하며 지리 기반의 라우팅과 보안 및 생존력이 강한 통신망의 구성을 목표로 현재는 프로젝트가 완료된 상태이다.

4. Ad-Hoc 라우팅 프로토콜에서의 보안

4.1 Ad-Hoc 네트워크 보안을 위한 고려 사항

Ad-Hoc 네트워크는 기본적으로 망 내의 모든 노드에 데이터를 전송하는 브로드 캐스팅 방식을 사용한다. 망 내부의 모든 노드는 다른 노드로의 송/수신 데이터 내용을 청취할 수 있기 때문에 의도된 수신자 이외의 다른 노드에게 데이터가 노출될 위험이 있다. 또한 매체를 신뢰할 수 없는 Ad-Hoc 네트워크의 특성상 암호를 사용할 수 없기 때문에 암호 키 방식에 크게 의존하게 되므로, 키 간에 신뢰할 수 있는 관계를 형성하고 이를 네트워크 전반에 분배하는 것이 주요한 보안 이슈라고 할 수 있다. 그러나 Ad-Hoc 네트워크에서의 보안에 관한 연구는 아직 미흡한 실정이다.

본 고에서는 Ad-Hoc 네트워크에서 제기될 수 있는 보안 이슈 및 보안을 지원하기 위해 제안된 몇몇 프로토콜에 관해 살펴보려 한다.

Ad-Hoc 네트워크에서도 기존 유선 네트워크에서의 보안과 마찬가지로 기본적으로 다음과 같은 사항을 고려해 볼 수 있다.

첫 번째로는 가용성(Availability)에 관한 문제로, 가용성이란 권한 있는 사용자가 원하는 자료를 적시에 제공받을 수 있도록 하는 특성이다. 그러나, 가용 주파수 대역 경쟁 및 제한된 배터리 소비를 유발하는 공격에 의해 가용성이 보장되지 못할 수 있다.
그러므로 자원예약 메커니즘을 바탕으로 불필요한 접속을 제한하고, 우선순위 서비스를 제공하여 가용성을 보장하는 방안을 고려해 볼 수 있다.

두 번째는 인증(Authenticity)에 관한 사항이다. 인증이란 자신이 보낸 정보가 의도된 상대방에게 정확히 전달되어 이용되는가를 판단하는 것으로, 정보의 변경이나 위조 없이 본래의 정보 그대로 임을 보증하는 메시지 인증과, 특정 사용자가 바로 그 사용자임을 보증하는 사용자 인증으로 구분할 수 있다. 인증은 가장 필수적인 선행조건이나 Ad-hoc 네트워크에서는 매체를 신뢰할 수 없다는 특징이 있으므로 신뢰할 수 있는 제 3 자 증명(certification)의 도움 없이 키들 간에 신뢰할 수 있는 관계를 정립하는 것이 핵심적인 사항이라고 할 수 있다.

세 번째로는 무결성(Integrity)에 관한 문제이다. 무결성은 정당한 권한을 갖지 않은 자에 의해 정보가 변경 또는 삭제되지 않도록 보호하여 정보의 완전성, 정확성을 보장하는 특성을 의미한다. 정보가 이미 변경되었거나 변경의 위험이 있을때 이를 복구할 수 있는 메커니즘이 필요하다.

마지막으로는 비밀성(Confidentiality)에 관한 문제로, 비밀성이란 정보의 소유자가 의도한 대로 정보의 비밀을 유지하며 인증 받은 사용자의 접근만을 허용하여 인가되지 않은 정보의 공개를 방지하는 특성이다. 물리적 수준 혹은 네트워크 수준에서의 접근통제가 가능하며 접근통제에 실패했을 경우에도 데이터가 암호화되어 있다면 비밀성의 유지는 가능하므로, 데이터 암호화에 관한 사항이 고려될 수 있다. 그러나 암호화 키 사용 시, 저전력에 자원의 사용에 제약이 있는 Ad-Hoc 네트워크에서 키를 암호화 하고 복호화 하는 과정에 생기는 오버 헤드에 관한 문제점이 발생할 수 있다. [6]

위에서 언급한 보안 이슈의 적용을 위해 Ad-Hoc 네트워크 분야에서는 잠재적인 공격에 대처할 수 있는 강건한 라우팅 프로토콜의 설계를 연구하는 Secure Routing, 인프라가 없는 환경에서의 키 분배 및 관리방안에 관한 연구, 침입탐지 및 대처 방안에 관한 연구가 진행되고 있으며 본 고에서는 Secure Routing 에 관한 연구를 중점적으로 살펴보고자 한다.

4.2 Ad-Hoc 네트워크의 Secure Routing 프로토콜

Ad-Hoc 네트워크에서의 라우팅 프로토콜은 네트워크 내의 노드들이 멀티 홉 경로, 즉 하나의 목적지에 대해 다양한 경로를 설정하여 Load Balancing, Redundancy 기능을 제공할 뿐 아니라 이를 바탕으로 더 나은 Throughput 을 제공하여 네트워크의 효율성을 높일 수 있도록 해야 한다. 또한 네트워크 위상이 빈번하게 변하는 Ad-Hoc 네트워크에서 노드간의 연결을 유지하기 위해 변화에 능동적으로 대응하고 새로운 경로를 학습할 수 있도록 해야 하며, 경로 정보의 교란과 같은 악의적인 공격으로부터 네트워크를 보호해야 한다. 그러나 Ad-Hoc 네트워크의 동적인 특성과 자원의 제약으로 인해 적절한 프로토콜의 설계가 쉽지 않다.

Ad-Hoc 네트워크 라우팅 프로토콜은 일반적으로 불필요한 추가 패킷을 삽입하여 한정된 대역폭이나 계산 자원을 소비하도록 하거나, 라우팅 루프, 블랙홀, 웜홀과 같이 정당한 데이터 패킷을 장애가 있는 경로로 라우팅 하거나, 경로 탐색 요청 패킷을 미리 유포하여 후에 정당한 라우트 요청 패킷을 중복 패킷으로 간주하게 하여 탐색 요청을 무시하도록 하는 공격을 받을 수 있다.

즉, Ad-Hoc 네트워크는 공격에 취약하기 때문에 도청이 용이하고, 잘못된 라우팅 정보를 바탕으로 한 Replay 공격이나 정보의 왜곡이 발생하기 쉽다. 또한 중앙 집중적인 구조가 아닌 분산 네트워크 구조로, 위상이 동적으로 변경되기 때문에, 변경된 노드의 상태를 즉시 반영할 수 있는 확장성 있는 보안 메커니즘이 요구된다.

Ad-Hoc 네트워크의 이러한 특성을 기존의 Ad-Hoc 라우팅 프로토콜에 반영한 Secure Routing 프로토콜로 제안된 프로토콜은 다음과 같다.

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

SAR[7]은 인프라의 지원없이 전원, 메모리, 프로세싱 처리능력과 같은 자원의 사용이 제한적인 Ad-Hoc 네트워크에서 보안을 제공하기 위한 라우팅 프로토콜로서 제안된 방식이다. 기존의 Ad-Hoc 라우팅 프로토콜은 보안에 대한 고려 없이 홉 사이의 거리를 기준 값으로 사용하여 경로를 설정하였다. 그러나 Ad-Hoc 네트워크에서 보안 문제를 프로토콜에서 지원하기 위하여 SAR 에서는 일반적인 라우팅 메트릭 요소로 노드의 보안 레벨을 포함하는 방식을 사용한다.

SAR 은 On-demand 라우팅 방식인 AODV 의 기본 동작절차를 바탕으로 하여 경로탐색을 요청하는 RREQ 와 그에 대한 응답인 RREP 패킷 내에 보안 메트릭 값을 내장하는 방식을 사용한다.

SAR 에서는 라우팅 프로토콜의 여러 메트릭 요소 중 패킷 전송순서는 시퀀스 번호가 담당하고, 인증은 비밀번호와 인증서가, 무결성은 메시지 다이제스트와 전자서명이, 기밀성은 암호화를 통해 지원한다.

동작 절차는 다음과 같다.

먼저 RREQ 내의 RQ_SEC_REQUIREMENT 라는 추가 필드는 목적지까지의 경로에서 요구하는 보안 레벨을 알려준다. 경로의 중간 노드의 보안 레벨이 요구된 보안 레벨보다 낮을 경우에 RREQ 패킷은 폐기되며, 목적지에 RREQ 의 도착은 해당 목적지까지의 경로의 보안 레벨이 RQ_SEC_REQUIREMENT 필드내의 보안 레벨을 만족하는 경로, 즉 Secure Route 임을 의미한다.

RREQ 의 RQ_SEQ_GUARANTEE 필드의 값은 RREP 의 RP_SEQ_GUARANTEE 필드로 복사되며, RREP 패킷이 역 경로의 중간노드에 도착하면 라우팅 테이블은 새로운 RP_SEQ_GUARANTEE 값으로 업데이트 된다.

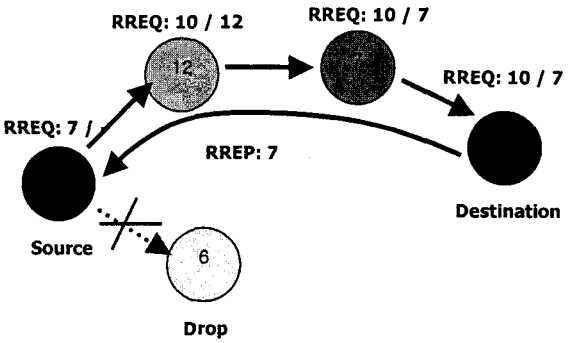

그림 1 .SAR 의 동작과정
(보안 레벨 수준을 만족시키지 못하는 RREQ 메시지는 폐기됨)

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

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

Ad-Hoc 네트워크의 보안 관련 프로토콜로 제안된 SEAD[8]는 Table-driven 라우팅 프로토콜인 DSDV 를 기반으로 단방향 해시 체인을 사용하여 Ad-Hoc 네트워크에 인증과 데이터 무결성을 제공하는 프로토콜이다.

단방향 해시 체인은 단방향 해시 함수를 사용하며, 계산과정이 단순하고 입력값에 매우 종속적이기 때문에 입력값에 따라 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 사용되며, 데이터의 무결성을 지원한다.

SEAD 를 적용하는 네트워크 내의 모든 무선링크는 양방향임을 가정하며, 패킷의 손실이나 복사, 전송 순서의 변경 및 자원사용의 제약과 같은 Ad-Hoc 네트워크의 기본 특성을 바탕으로 설계되었다. SEAD 는

DSDV 를 기반으로 하기 때문에 목적지 시퀀스 번호를 사용하여 라우팅 루프의 발생을 막고 라우팅 업데이트 메시지의 Replay attack 을 방지한다.

SEAD 는 간단한 암호화 기법을 사용하기 때문에 처리 능력과 대역폭등의 자원이 제한된 Ad-Hoc 네트워크에서 효율적으로 기밀성을 보장하며, Table-driven 방식의 라우팅 프로토콜 외에 On-demand 방식의 라우팅 프로토콜에도 적용하기 위한 방안에 관한 연구가 계속되고 있다.

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

Ad-Hoc 네트워크에서의 Secure Routing 을 지원하기 위해 제안된 프로토콜인 Ariadne[9]은 on-demand 방식의 프로토콜인 DSR 을 기반으로 하며 대칭키를 사용하는 보안관련 프로토콜이다..

Ariadne 에서는 pair-wise 공유 비밀키와 TESLA, 디지털 서명 세가지의 키 설정 메커니즘이 사용될 수 있다. 이 중 TESLA 는 멀티캐스트 통신에서 각 패킷의 인증을 정의하는 인증방식으로 계산적 과부하가 적은 해쉬 함수를 사용하고 시간 지연적 키 노출 방법을 사용하여 각 패킷의 인증을 수행한다. 송신자는 인증키를 키 노출 시간이 지난 후에 전송 패킷에 실어보내며, 수신자는 그 노출 시간이 지난 후에 이전에 받은 패킷을 인증할 수 있다. 인증키는 단방향 키 체인을 사용하여 역방향으로 계산되므로 중간에서 임의로 생성할 수 없으며 패킷의 손실에 강한 장점이 있다.

일반적으로 Ad-Hoc 네트워크는 라우팅 프로토콜을 이용하여 정당한 데이터 패킷을 장애가 있는 경로로 라우팅 하여 라우팅 루프나, 블랙홀을 생성하는 라우팅 분열 공격방식과 패킷을 추가적으로 삽입하거나 DoS 공격을 통하여 대역폭과 프로세싱 자원을 소비하게 하는데, Ariadne 은 TESLA 를 라우팅 경로내의 노드를 인증하는데 사용하여 계산과 통신에 따르는 오버헤드를 줄이고, DoS 공격을 방지한다.

Ariadne 는 경로 복구 과정시 Route Request 의 목적지 노드를 인증하고 Route Request 와 Route Reply 가 전송되는 경로내의 노드를 인증하기 위해 TESLA 와 대칭키를 공유 및 디지털 서명 방식을 사용한다. 홉단위의 해싱을 통해 경로내에서 누락된 홉이 없음을 검증하여 Secure Routing 을 보장한다.

Ariadne 의 사용을 통하여 목적지까지의 경로 중 협의되지 않은 노드가 존재할 경우 Route Reply 내의 정보를 바탕으로 협의되지 않은 경로를 따라서 패킷을 전송할 수 있게 한다. 또한 홉 단위로 해싱한 인증코드를 사용하며 TESLA 의 최대 종단 지연 특성과 해시 체인을 사용하여 외부의 공격으로부터 네트워크를 보호할 수 있다. Ariadne 은 DSR 을 기반으로 하고 있으나 향후 최적화된 DSR 에도 적용할 수 있도록 하는 연구가 진행되고 있다.

5. 결론

Ad-Hoc 네트워크에서는 라우팅 프로토콜의 역할이 매우 크다. 이는 네트워크 위상이 동적으로 변하고, 배터리와 CPU 같은 자원이 제한되어 있는 Ad Hoc 네트워크에서 불필요한 자원의 낭비를 막고, 효율적인 네트워크를 구성하기 위해서 이다.

Ad-Hoc 네트워크에서는 라우팅 프로토콜을 이용한 공격이 많이 발생하기 때문에 라우팅 프로토콜 설계시 보안에 관한 사항을 고려해야 한다.

Ad-Hoc 네트워크는 네트워크 특성상 보안이 취약하며 이를 보완하기 위해 라우팅 프로토콜을 비롯하여 암호 키 분배 및 관리 분야에서 많은 연구가 진행되고 있다.

본 고에서 소개한 보안관련 프로토콜은 극히 일 부분에 지나지 않으며 좀 더 다양한 각도에서 라우팅 프로토콜을 통한 Ad-Hoc 네트워크의 보안을 보장하기 위한 연구가 지속되어야 할 것이다.

[참고문헌]

[1] 2001, " Ad-Hoc Networking" Charles E. Perkins .Addison Wesley

[2]http://www.ietf.org/rfc/rfc3561.txt

[3]http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[4]http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-11.txt

[5]http://www.ietf.org/internet-drafts/draft-ietf-manet-tbrpf-10.txt

[6] 1999, IEEE Network Magazine, L.Zhou, Z.J.Hass

[7]2001,UIUCDCS-R-2001-2241,UILU-ENG-2001-1748, Seung Yi et al

[8] 2002,WMCSA, Yih-Chun Hu, David B. Johnson, Adrian Perrig

[9] 2002, MobiCom, Yih-Chun Hu, David B. Johnson, Adrian Perrig