Ad-Hoc 네트워크를 위한 효율적 Routing 프로토콜

김민정[O] 김기천, 성연주
건국대학교 컴퓨터공학과
{mjkim[O], kckim, yjsung }@konkuk.ac.kr

Efficient Routing Protocol for Ad-Hoc Nework

Minjeong Kim[O], Keecheon Kim, Younju Sung
Dept. of Computer Science , Konkuk Univ.

Ad-Hoc 네트워크에서는 노드의 위상 변화가 빈번히 발생하므로 경로 탐색 및 관리가 중요하다. 그러나 자원의 사용이 제한된 무선망에서 경로 탐색과 관리에 많은 자원을 소비하게 되면, 데이터 처리시의 자원사용에 영향을 미치게되므로 네트워크의 효율이 저하된다. 효율적인 Ad-hoc 네트워크를 구성하기 위해서는 효율적인 라우팅 프로토콜의 설계가 매우 중요하다. 현재 표준으로 제정된 Ad-Hoc 라우팅 프로토콜들과 그 개선방안에 대해 살펴보고, 보안에 취약한 Ad-Hoc 네트워크에서 보안성을 제공하기 위해 제안된 프로토콜에 관해 살펴본다.

1. 서 론

Ad-hoc 네트워크는 기존 유선 네트워크 환경에서 제공하는 통신 인프라가 존재하지 않는 곳에서 단말기 간의 라우팅 만으로 데이터의 송수신을 수행하는 무선 네트워크[1]로, 연구 초기에는 군사적인 목적으로 개발되었다. Ad-Hoc 네트워크 내의 단말기는 단말로서의 기능 뿐 아니라 라우터, 서버의 역할을 수행하여 네트워크 내의 단말들의 동적인 상태 및 위상 변화를 실시간으로 반영하여 통신을 지원한다.

무선 네트워킹 분야의 급속한 기술 발달로 인해 Ad-Hoc 네트워크에 대한 요구사항 및 적용범위는 점점 증가하고 있는 추세이며, 차세대 네트워크라고 일컬어지는 유비쿼터스 컴퓨팅 분야에서도 역시 효율적인 Ad-Hoc 네트워크 구성이 필수적이다. 따라서 무선 네트워크의 기반 기술로서의 Ad-Hoc 네트워크의 중요성이 증대되고 있으며, 많은 연구기관에서 관련 연구가 추진되고 있다.

본 논문에서는 Ad-Hoc 네트워크의 라우팅 프로토콜 및 개선 방안을 살펴보고, 보안에 취약한 Ad-Hoc 네트워크를 보완하기 위해 제안된 몇몇 보안 라우팅 프로토콜에 관해 살펴보고자 한다.

2. Ad-Hoc 네트워크 라우팅 프로토콜

2.1 Ad-Hoc 네트워크의 특징

Ad-Hoc 네트워크는 중앙의 통제로부터 완전히 독립하여 사용자로 하여금 더 많은 자유와 유연성을 확보할 수 있도록 하며, 네트워크의 구성과 이동이 용이한 특징이 있다.

Ad-Hoc 네트워크는 기존 인프라의 지원 없이 보안 및 라우팅 기능을 수행하여야 하며, 관리를 담당하는 중앙노드가 없기 때문에 각각의 기능을 네트워크 내의 노드에 분산시켜 수행한다. 또한 네트워크의 위상이 빈번하게 변하므로 노드의 상태를 반영하는 다양한 네트워크 형태를 구성할 수 있으며, 네트워크의 위상 변화에 관계없이 지속적으로 서비스를 제공할 수 있어야 한다. Ad-Hoc 네트워크 내의 노드들은 불필요한 자원낭비가 발생하지 않도록 효율적인 알고리즘과 메커니즘을 적용하여 최소한의 자원사용으로 최대한의 성능을 목표로 하며, 일반적으로 고정망에 비해 정보와 물리적 보안 위협에 더 많이 노출되어 있으나 이를 보완하기 위한 관련 연구는 아직 미흡한 실정이다.

2.2 Ad-Hoc 네트워크 라우팅 프로토콜

2.2.1. Table-Driven(Proactive) 방식

Table-Driven 방식은 Bellman-Ford 방식을 기초로 Ad-Hoc 네트워크 내의 각 노드가 도착 가능한 모든 노드들의 라우팅 정보를 라우팅 테이블에 유지하는 방식으로, 빠른 경로 획득이 장점이다. 그러나 라우팅 정보를 갱신하기 위한 주기

적인 방송 메시지와 라우팅 정보의 교환은 무선 대역의 낭비를 초래하며 이로 인해 네트워크의 성능저하를 유발한다. DSDV(Destination Sequenced Distance Vector)가 Table-Driven 방식에 해당되며, Bellman-Ford 방식을 기반으로 목적지 순차 번호(Destination Sequence Number)를 사용하여 라우팅 루프의 발생을 방지한다.

2.2.2 On-Demand (Reactive) 방식

On-demand 방식은 경로 요청시에만 경로 획득 절차를 수행하여 불필요한 오버헤드 발생을 줄일 수 있다. 그러나 데이터 전송을 위해서는 경로 획득 절차가 먼저 수행되어야 하므로 데이터 전송까지의 지연시간이 길다는 단점이 있으나 노드의 이동이 빈번한 Ad-Hoc 네트워크에 적합한 라우팅 방식으로 AODV, DSR 등이 포함된다.

DSR(Dynamic Source Routing)[2]은 소스 라우팅 방식을 기반으로 하며, 네트워크 내의 모든 노드는 라우트 캐쉬를 유지한다. DSR은 RREQ(RouteRequest)/RREP(Route Reply) 메시지를 사용하는 경로 탐색 절차와 RERR(Route Error) 메시지를 사용하는 경로 관리 절차로 이루어진다. AODV(Ad hoc On-Demand Distance Vector)[3]는 DSDV와 같이 목적지 순차 번호를 사용하여 라우팅 루프를 방지하며, DSR과 유사한 경로 탐색 절차를 사용한다. 경로 탐색시 RREQ 메시지를 이웃 노드로 브로드캐스팅 하면, 목적 노드로의 경로 정보를 가진 노드가 RREP 메시지를 소스 노드에 전송한다.

2.2.3.Hybrid 방식

ZRP(Zone Routing Protocol)는 Table-Driven 방식과 On-Demand 방식을 혼합한 방식으로서 미리 정의된 라우팅 영역(zone)을 기반으로 영역 내부에서는 IARP (Intrazone Routing Protocol)이, 외부에서는 EARP (Extrazone Routing Protocol)이 라우팅 정보를 관리한다.

2.2.4. 기타

이 외에도 노드의 에너지 상태를 고려한 Power-Aware Routing(PAR), 위치 정보를 이용한 Location-Aware Routing(LAR), 경로의 지속성을 고려한 Associativity-Based Long-lived Routing(ABR) 프로토콜 등이 있다.

Ad-Hoc 네트워크 내의 경로는 노드들의 동적인 위상변화로 인해 경로 탐색과 경로 복구 과정이 빈번하게 발생하는데, 이에 소요되는 시간을 단축할 수 있다면 노드들의 위상 변화에 신속하게 대응할 수 있게 될 뿐 아니라 효율적인 경로를 통해 데이터 전송을 빠르게 할 수 있으며, 경로 탐색과 경로 복구 과정 동안에 유실되는 데이터를 줄임으로서 네트워크의 신뢰성을 높일 수 있게 된다. DSR의 경우 네트워크 내의 모든 노드는 라우트 캐쉬를 유지하고 있으므로, 경로 재구성을 위한 탐색을 소스 노드부터 하는 것이 아니라 에러가 발생한 노드에서부터 시작하면 경로 재구성에 소요되는 시간을 단축할 수 있다. AODV는 목적지 순차번호를 사용하므로 이를 이용하여 경로의 손실시에 노드가 유지하고 있는 정보의 목적지 순차번호를 확인하여 경로 탐색의 수행 여부를 판단하여 불필요한 경로 탐색의 횟수를 줄임으로서 경로 복구에 걸리는 시간을 단축할 수 있다.

3. Ad-Hoc 네트워크의 Secure Routing 프로토콜

Ad-Hoc 네트워크는 망 내의 모든 노드에 데이터를 전송하는 브로드캐스팅 방식을 사용한다. 이것은 무선 네트워크의 특성으로, 데이터의 전송이 물리적 매체가 아닌 대기를 이용하기 때문이다. 망 내부의 모든 노드는 다른 노드로의 송/수신 데이터 내용을 청취할 수 있기 때문에 의도된 수신자 이외의 다른 노드에게 데이터가 노출될 위험이 크다. 그러나 Ad-Hoc 네트워크에서의 보안에 관한 연구는 아직 미흡한 실정이다. Ad-Hoc 네트워크에서의 보안도 기존 유선 네트워크와 마찬가지로 다음과 같은 사항을 고려한다.

가용성(Availability)은 권한 있는 사용자가 원하는 자료를 적시에 제공받을 수 있도록 하는 것으로, Ad-Hoc 네트워크에서는 제한된 자원의 낭비를 유발하는 공격에 의해 가용성이 보장되지 않을 수 있다. 그러므로 자원예약 메커니즘을 바탕으로 불필요한 접속을 제한하고, 우선순위 서비스를 제공하여 가용성을 보장하는 방안을 고려해 볼 수 있다. 인증(Authenticity)은 자신이 보낸 정보가 의도된 상대방에게 정확히 전달되어 이용되는가를 판단하는 것이다. 인증은 보안의 필수적인 선행조건이나 Ad-hoc 네트워크에서는 매체를 신뢰할 수 없다는 특징이 있으므로 신뢰할 수 있는 제3자 증명(certification)의 도움 없이 키 간에 신뢰할 수 있는 관계를 정립하는 것이 관건이다. 무결성(Integrity)은 정당한 권한을 갖지 않은 자로부터의 정보 변경을 보호하여 정보의 완전성, 정확성을 보장하는 것으로 정보가 이미 변경되었거나 변경의 위험이 있을 때 이를 복구할 수 있는 메커니즘이 필요하다. 기밀성(Confidentiality)은 인증 받은 사용자의 접근만을 허용하여 인가되지 않은 정보의 공개를 방지하는 특성이다. 물리적 수준 혹은 네트워크 수준에서의 접근통제가 가능하며 접근통제에 실패했을 경우에도 데이터가 암호화되어 있다면 비밀성

의 유지는 가능하므로, 이를 위한 데이터 암호화와 키의 암/복호화 과정에서 발생하는 오버헤드를 고려해야 한다.[4]

Ad-Hoc 네트워크는 도청이 용이하고, 외부로부터의 공격이나 정보의 왜곡이 발생하기 쉽다. 또한 동적인 위상 변경을 즉시 반영할 수 있는 확장성 있는 보안 메커니즘이 필요하다. Ad-Hoc 네트워크의 이러한 특성을 기존의 Ad-Hoc 라우팅 프로토콜에 적용하여 제안한 Secure Routing 프로토콜에는 다음과 같은 것들이 있다.

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

기존의 Ad-Hoc 라우팅 프로토콜은 경로선택 시 보안에 대한 고려 없이 홉수를 기준으로 사용해왔다. SAR에서는 일반적인 라우팅 메트릭 요소로 노드의 보안 레벨을 포함한다. SAR[5]은 On-demand 라우팅 방식인 AODV의 기본 동작절차를 바탕으로 하여 경로탐색을 요청하는 RREQ와 그에 대한 응답인 RREP 패킷 내에 보안 메트릭 값을 내장하는 방식을 사용한다. RREQ내의 RQ_SEC_REQUIREMENT 필드에는 경로에서 요구하는 보안 레벨을 포함하며, 요구된 보안 레벨보다 낮을 경우에 RREQ 패킷은 폐기되므로, 목적지에 RREQ가 도착하면, 목적지까지의 경로의 보안 레벨은 RQ_SEC_REQUIREMENT 필드내의 보안 레벨을 만족하는 경로, 즉 Secure Route임을 의미한다.

SAR은 이동 Ad-Hoc 환경에서 안전한 경로를 발견할 수 있게 하며, DSR이나 AODV와 같은 기존의 On-demand 라우팅 프로토콜에 쉽게 적용할 수 있다. SAR을 적용함으로서 발생하는 오버헤드는 RREQ/RREP 메시지의 플러딩 범위를 제한함으로서 감소시킬 수 있다.

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

SEAD[6]는 DSDV를 기반으로 단방향 해시 체인을 사용하여 Ad-Hoc 네트워크에 인증과 데이터 무결성을 제공하기 위해 제안된 프로토콜이다. 단방향 해시 체인은 계산과정이 단순하고 입력값에 따라 어떤 결과 값이 나올지 전혀 예측할 수 없으며, 결과 값으로부터 입력값을 계산해 낼 수 없으므로 메시지 암호화를 통해 데이터의 무결성을 지원하기 위해 사용된다. SEAD는 DSDV를 기반으로 하기 때문에 목적지 순차 번호를 사용하여 라우팅 루프의 발생을 방지하고 라우팅 업데이트 메시지의 Replay 공격을 예방한다. SEAD는 간단한 암호화 기법을 사용하기 때문에 처리 능력과 대역폭등의 자원이 제한된 Ad-Hoc 네트워크에서도 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)

Ariadne[7]은 DSR을 기반으로 대칭키를 사용하는 보안 관련 프로토콜이다. Ariadne에서는 TESLA를 사용하여 키를 인증하는데, TESLA는 멀티캐스트 통신에서 각 패킷의 인증을 정의하는 인증방식으로, 계산적 과부하가 적은 해쉬 함수를 사용하고 시간 지연적 키 노출 방법을 사용하여 각 패킷의 인증을 수행한다. 인증키는 단방향 키 체인을 사용하여 역방향으로 계산되므로 중간에서 임의로 생성할 수 없으며 패킷의 손실에 강한 장점이 있다.. Ariadne은 DSR을 기반으로 하고 있으나 향후 최적화된 DSR에도 적용할 수 있도록 하는 연구가 진행되고 있다.

5. 결론

효율적인 라우팅 프로토콜은 Ad-Hoc 네트워크에서 매우 중요하다. 이는 네트워크 위상이 동적으로 변하고,자원의 사용이 제한되어 있는 Ad Hoc 네트워크에서 불필요한 자원의 낭비를 막고, 효율적인 네트워크를 구성하기 위한 것이다. 이를 위해 경로 설정과정의 메시지 교환 횟수를 줄이고, 자원의 사용을 최소화 하며 시간을 단축하는 방향으로 기존의 라우팅 프로토콜을 개선하는 방법이 제안되고 있다. 또다른 고려사항은 보안이다. Ad-Hoc 네트워크는 네트워크 특성상 보안이 취약하며 이를 보완하기 위해 라우팅 프로토콜 및 암호 키 분배 및 관리 분야에서 관련 연구가 진행되고 있다. 본 고에서 소개한 라우팅 프로토콜은 극히 일부분이며, 앞으로 더 다양한 관점에서 보안을 보장할 수 있는 라우팅 프로토콜에 관한 연구가 지속되어야 할 것이다.

[참고문헌]

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

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

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

[4] 1999, IEEE Network Magazine, L.Zhou, Z.J.Hass

[5] 2001,UIUCDCS-R-2001-2241,UILU-ENG-2001-1748, Seung Yi et al

[6] 2002,WMCSA, Yih-Chun Hu, David B. Johnson, Adrian Perrig

[7] 2002, MobiCom, Yih-Chun Hu, David B. Johnson, Adrian Perrig