애드혹 네트워크의 인증서 체인 상에서 노드간 안전한 경로 탐색기법에 관한 연구

°최성재* 양대헌** 송주석*
연세대학교 컴퓨터과학과*, 인하대학교 정보통신대학원**
{ntchoi°, jssong}@emerald.yonsei.ac.kr*, Nyang@inha.ac.kr**

A Study on the Finding the Effective path on Certificate-Chains in MANETs(Mobile Ad Hoc Networks)

Sungjae Choi* . JooSeok Song* DaeHun Nyang**
Department of Computer Science Yonsei University*,
Graduate School of Information Technology & Telecommunication Inha University**

요 약

애드혹 네트워크(Ad hoc networks)에서 각 노드는 자유로이 이동하며, 이러한 변화에 맞춰 매 번 각 노드 간에는 새로운 신뢰관계가 형성되어야 한다. 이와 같은 시스템에서 토폴로지의 변화에 따른 정보를 빠르게 획득하는 것은 물론이거니와 이에 수반되는 노드 간 라우팅 경로를 안전하게 형성하는 것은 애드혹 네트워크 환경에서는 매우 중요한 부분이다. 이에 본 논문에서는 애드혹 네트워크 환경에서 효율적인 플러딩(flooding) 기법을 사용하여 최적의 인증서 체인(certificate-chain)을 안전하게 구축하는 방법을 제안하고자 한다. 이는 노드들이 잦은 이동성으로 인해 극심한 토폴로지 변화에도 효율적으로 신뢰 관계를 유지하도록 하며, 효과적인 플러딩 방식을 사용하여 최소의 시간 동안 최적의 인증서 경로를 찾아내는 방식이다.

1. 서 론

기지국이나 AP(Access Point)등 어떤 기존 네트워크 인프라도 갖지 않는 애드 혹 네트워크의 보안 목표는 주로 안전한 라우팅(secure routing), 키 운영(key management) 및 분산 서비스(distribution service), 인증(authentication), 노드들 사이의 협력, 모바일 디바이스 보안(mobile device security)등에 관해서 연구가 되고 있다.

그러나 이러한 보안 목표를 달성하기 위해 현재까지 진행된 Security 관련 연구 중에는 노드들 간의 신뢰관계를 가장 효율적으로 찾아내고, 이를 유지하고자 하는 연구가 없다. 이에, 본 논문은 이러한 애드 혹 네트워크 환경에서의 라우팅 프로토콜 방식이, 그 환경에서 각 노드들 간의 신뢰 관계에서 형성된 인증서 체인[1] 에서, 새로이 신뢰 관계를 형성하고자 하는 노드를 찾고자 하는 탐색 과정과 유사함을 발견하였고, 애드 혹 환경에서의 라우팅 방식을 Security의 관점에서 노드들의 신뢰 관계형성 과정에 적용해 보았다.

애드 혹 네트워크의 모든 노드는 1 홉 떨어진 인접 노드들의 정보를 알고 있다. 이에 보안적인 측면에서 다음과 같은 가정을 하고자 한다. 애드 혹 네트워크의 각 노드가 인접 노드들과 정기적인 폴링을 통해 정기적으로 인증서 교환이 이루어져 신뢰관계가 형성되어 질 수 있다고 하자. 이렇게 모든 노드들이 그들로부터 1홉 떨어진 모든 노드들과 신뢰 할 수 있는 관계가 형성되어 있다면 한 노드가 그 인접 노드들을 신뢰하고 또 그 인접 노드는 또 그 인접 노드들을 신뢰하는 과정을 통해 여러 경로의 신뢰 관계로 맺어진 체인이 형성 될 수 있는 데 이렇게 형성된 여러 경로들 중에서 최적의 인증서 체인의 경로를 찾는 방법은, 애드 혹 네트워크에서 라우팅 경로를 찾는 방식과 비슷하다고 할 수 있다.

애드 혹 네트워크의 라우팅 방식 중 프로엑티브 (proactive)방식으로 경로를 찾을 경우 주기적인 라우팅 정보를 브로드캐스팅(broadcasting) 하므로 인해 무선 대역폭의 낭비가 많으며, 빈번한 이동성을 갖는 애드 혹 특성 때문에 라우팅 패킷의 부하가 증대되는데, 특히 노드수가 많아 질 수록 이 부하의 정도는 더 심각하다. 이러한 프로엑티브의 문제점들로 인해 본 논문에선 경로를 찾는 방법을 리엑티브(reactive) 방식의 대표적 방법의 하나인 AODV(Ad hoc On-Demand Distance Vector Routing)[2] 방식을 이용하여 출발지에서, 안전한 통신을 하고자 하는 목적지까지의 신뢰관계를 찾아보았다. 그러나 물론, 이 AODV 방식도 여러 가지 문제가 있는데 대표적인 문제는 플러딩이다. 기존의 프로엑티브 방식에서 일어나는 플러딩의 가장 중요한 문제는 비용 및 효율성의 측면과 불필요한 대역폭의 낭비에서 많은 문제점이 있어 기본적으로는 AODV가 목적지 노드를 찾아가는 방법을 이용하되 플러딩 방식에 있어서는 수정된 방식[11],[12]을 사용하고자 한다. 이러한 방식의 기본적인 생각은 Williams, B.와 Camp, T가 분류한 4개의 프로토콜 그룹[3]중 헬로우 패킷 (Hello packet) 을 통해 재 브로드캐스팅(re-broadcasting)을 판단하여 각 노드의 이웃상태를 유지하는 Neighbor Knowledge Methods를 사용하였다. 이러한 방법들의 근본적인 생각은 1홉 떨어진 노드가 그 주위 노드의 정보를 알고 있으므로, 결과적으로 한 노드는 2홉 떨어진 노드들의 정보까지 알게 되는 것과 같게 되어, 무조건 브로드캐스팅 하는 전통적 플러딩 방식보다는 효과적으로 경로를 찾을 수 있는 방법이다. 특히 이 방법들 중 Dominant-pruning(DP)[4], Total Dominant-pruning(TDP)[5] 플러딩 방식을 적용하여 애드 혹 환경에서의 인증서 체인을 찾기 위한 패킷 플러딩의 효율성을 높였다. 본 논문의 구성은 최적의 인증서 체인을 찾기 위한 구조를 시스템의 초기화 단계와 최적의 인증 경로 탐색단계로 제안한다.

2. 효율적인 인증경로 탐색과정

본 논문의 목적은 MANETs 환경에서 인증서 체인을 효과적으로 찾기 위한 것인데, 제안하는 모델의 기본적 운영을 위해 MANETs의 모든 노드들은 자신에게서 인접한 노드들을 신뢰한다고 가정하자. 이러한 가정은 한 노드가 물리적으로 안전하고 짧은 거리의 사이드 채널(side channel) 즉 적외선 채널과 같은 채널을 통해서 키들을 교환했다고 보면 두 노드 사이는 신뢰할 수 있는 관계를 맺을 수 있다.

본 제안은 이러한 가정에 추가하여 시스템의 효율성을 위해 인접 노드들 간의 거리를 자신의 파워영역(power range[10])이 아닌, 자신으로

부터 1홉 이내의 노드들 사이로 제한 하고자 한다. 신뢰 관계가 형성된 각각의 노드들은 그들 간에 인증서를 발급하는 과정을 통해 시스템의 인증서 체인을 형성한다. 이렇게 형성된 환경에서 효과적인 플러딩을 통해 인증서 체인을 찾고, 찾아진 경로를 이용해 출발지(source)와 목적지(destination)간의 신뢰관계를 형성하여 안전하게 통신할 수 있는 준비를 하는 것이 본 제안의 목적이다. 이를 위해 시스템 초기 설정 과정을 먼저 설명하고, CRREQ (Certificate-chain Routing REQuest) 송신과 CRREP (Certificate-chain Routing REPly) 수신과정을 통해 최적의 인증서 체인을 찾고자 한다. 각 단계의 상세한 내용은 아래에서 설명한다.

2.1 시스템 초기화

초기에 시스템을 운영하기 위해 설정해야 하는 것은 크게 3가지 단계를 거친다. 먼저, 첫 번째 단계는 인증서를 발행하는 단계로, 1홉 거리만큼 떨어져 있는 노드 A, B가 있다고 가정하자. 이때 1-홉 떨어져 있으며, 안전한 채널을 갖고 있는 A와 B는 서로의 인증서를 각각이 발행한다. 즉, A는 B의 인증서, 「A<<B>>」를 발행하고 B도 A의 인증서, 「B<<A>>」를 발행한다.

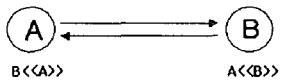

그림 1. 인증서 발행

이렇게 발행된 인증서에는 상대방의 정보(예, 상대방의 공개키, 상대의 이름, 유효 기간등)가 발행자의 개인키를 이용해 해쉬된 서명을 포함하여 신뢰할 수 있는 정보가 된다. 이러한 발행 과정은 시스템의 모든 노드들이 인접 노드들에 대한 인증서의 발행이 끝나는 시점까지 이루어진다. 이러한 발행과정이 끝나면 전체 시스템은 정상적으로 동작할 준비가 된다.

인증서의 발행이 끝나게 되면, 두 번째 단계로는 발행된 인증서의 교환이 이루어진다. 이 단계에서 각각의 노드들은 인접 노드들로부터 받아서 저장하고 있는 인증서들을 주기적으로 교환하게 된다. 이러한 교환 과정은 자신으로부터 1홉 반경이내에 있는 노드들 사이로 제한되며, 1홉 떨어진 인접 노드가 저장하고 있는 인증서의 목록에 변경이 있는 경우에만 교환 과정이 일어난다. 인증서의 교환주기는 각 노드들이 갖고 있는 타이머에 의해 미리 정해진 주파수 대역으로 정기적으로 헬로우 패킷을 교환함으로써 MANET의 이동성에 적절히 운용될 수 있도록 주기적으로 인증서 테이블 목록의 갱신이 이루어진다.

마지막 단계인 인증서 저장은 두 가지 방식에 의해 동작하는데 하나는, 각각의 노드가 자신으로부터 1홉 떨어진 인접 노드와 정기적으로 교환한 인증서를 자신의 인증서 테이블에 저장하는 방법이 하나 있고, 또 하나는 한 노드에서 통신하고자 하는 임의의 노드 간의 경로 탐색과정에 의해 찾아진 인증서 체인 상에 존재하는 노드들의 인증서를 가져와 저장하는 방법이다. 물론, 인증서 테이블 목록의 갱신도 인접 노드와의 정기적 교환 및 플러딩에 의한 최적의 인증서 체인의 경로를 통해 찾아진 경로상의 인증서들에 의해서 이루어진다.

2.2 최적의 인증경로 탐색

먼저, 출발지 노드는 자신이 목적지 노드의 인증서가 자신의 인증서 테이블 목록에 존재하는지 찾아본다. 여기서의 인증서 테이블은 출발지에서 목적지까지의 인증서 체인상의 경로를 저장하기 위해 필요한 것으로, 인증서 테이블의 경로 정보는 이전에 얻어진 경로 정보에 대해서만 유지하고 , 얻어진 경로 정보도 이동성을 만족시키기 위해서 유효한 시간을 설정하여 유효성 여부를 결정한다. 다음은 인증서 테이블의 주요 항목이다.

- Destination IP address , Sequence Number
- Hop Count , Last hop Count, Next hop
- List of Precursors, Lifetime
- Routing Flag, Interface

인증서 체인에서 경로를 찾기 위해 제일 먼저 할 일은 통신하고자 하는 목적지를 향해서 CRREQ(Certificate-Chain Routing Request) 패킷을 브로드 캐스팅 하는 것이다. 출발지 노드에서 이 패킷을 브로드캐스팅 할 때는 일단 자신이 원하는 목적지 노드에 대한 정보를 패킷에 실어 단순히 이웃 노드들에게 전송을 하면 된다.

2.2.1 CRREQ 수신

CRREQ 패킷을 처음 받은, 출발지 노드로부터 1홉 떨어진 노드들은 수신한 패킷을 전송하기 전에 자신이 이 패킷을 이전에 전송 받았는지 확인한 후 자신이 이전에 이 패킷을 받았으면 패킷을 버리고, 그렇지 않고 새로 받은 패킷이면 자신 주위에 목적지 노드가 있는지 여부와 목적지까지의 인증서 체인상의 경로가 존재하는지 여부를 판단하여 처리한다. 이때 자신에게 목적지 노드에 대한 정보가 없으면 출발지 노드로부터 받은 패킷에 출발지 노드의 인증서를 추가하여 다시 플러딩 한다. 물론 1홉 떨어진 노드가 아닌 경우는 출발지 노드에 대한 인증서의 추가과정 없이 단순히 패킷을 인접 노드로 전송하면 된다. CRREQ 패킷의 구조는 그림 2와 같다.

Type	D	G	Reserved	Hop count
CRREQ ID				
Destination IP Address				
Destination Sequence Address				
Originator Ip Address				
Originator Sequence Number				
Next Path Node Ip Address				
Next Path Node Sequence Number				
Node's certificates				

그림 2. CRREQ(Certificate-chain Route Request) 패킷 구조

여기서 Reserved는 0으로 전송하고, 수신시는 무시되며, CRREQ ID는 이 패킷을 발생시킨 일련번호를 의미한다. 또한 hop count는 출발지로부터 CRREQ를 수신한 도메인 까지의 홉수를 의미하며 처음 출발시는 0으로 설정된다. 패킷을 전송시 일반적인 MANET의 라우팅 프로토콜은 단순히 패킷을 플러딩 하는데 여기서는 DP와 TDP방법을 통한 플러딩을 사용한다.

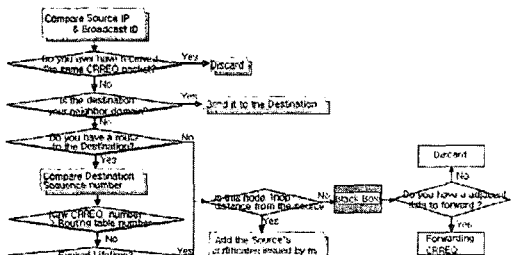

그림 3. CRREQ 전달 절차에 대한 알고리즘

이러한 과정들을 통해 목적지 노드가 CRREQ 패킷을 받으면 그 안에서 목적지 노드는 출발지 노드 의 인증서와 공개키를 신뢰할 수 있는 노드들을 통해 받을 수 있게 된다. CRREQ 패킷의 전달 절차에 대한 순서도는 그림 3과 같다. 여기서 'Black Box' 는 플러딩 하는 방법들을 의미하는 것으로 이 과정을 통해 플러딩 리스트를 획득한다.

2.2.2 CRREP 송신

출발지에서 전송한 CRREQ 패킷이 목적지에 도착하면, 목적지 노드는 CRREP(Certificate-chain Route Reply) 패킷을 생성한다. CRREP 패킷을 생성하는 경우는 목적지 IP Address가 직접 CRREQ 패킷을

수신한 경우와 CRREQ 패킷을 수신한 노드의 라우팅 테이블에 목적지 노드까지의 유효한 경로가 존재하는 경우다. 생성하는 절차 또한 각각의 경우에 따라 차이가 있는데 먼저, 목적지 노드에서 CRREP 패킷을 생성하는 경우는, Destination IP Address, Originator Ip Address, Originator Sequence Number를 CRREQ 패킷으로부터 복사해서 CRREP 패킷에 복사해 넣는다. 이 때 노드가 유지하고 있는 Destination Sequence Number의 마지막 일련 번호에 1을 증가시킨 값을 CRREP 패킷의 Destination Sequence Number에 저장하고 이를 축적된 path list를 참조로 CRREQ를 발생시켰던 노드 방향으로 유니캐스트(unicast) 한다.

Type	A	Reserved	APN Cnt	Prefix Sz	Hop count
Destination IP Address					
Destination Sequence Address					
Originator Ip Address					
Originator Sequence Number					
Next Path node Ip Address					
Next Path node Sequence Number					
node's certificates					

그림 4. CRREP(Certificate-chain Route Reply) 패킷 구조

이때 이 패킷을 전송하는 목적지 노드의 인증서를 패킷의 마지막에 추가하며, 이 패킷을 전송 받는 바로 인접 노드는 또한 자신의 인증서를 목적지 노드의 인증서에 추가한 후 다시 출발지 노드 방향으로 전송 하고, 출발지 노드까지 가는 경로 상에 있는 각 노드는 이렇게 계속 자신의 인증서를 CRREP 패킷에 추가한다. 이러한 인증서 추가과정을 다시 여러 노드들의 경우에서 살펴보면 그림-4와 같다.

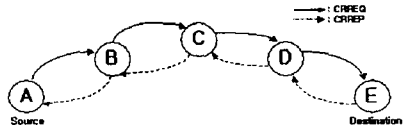

그림 4. CRREP 패킷의 전송

그림 4에서처럼, 출발지,A 와 목적지, E가 서로 신뢰된 상태에서 통신하고자 할 때, 제안하는 알고리즘은 3단계의 과정(three-way handshake)을 거친다.

먼저, 첫 번째 단계는 통신대상인 목적지를 찾는 단계이다. 만일, 출발지에서 전송된 패킷이 시스템의 많은 노드들을 거치는 과정에서 중간 노드들의 인증서를 추가한다면, 두 가지 문제점을 가져올 수 있다. 먼저, 시스템의 각 노드가 저장해야 하는 인증서의 수가 증가하게 되어 저장 공간의 낭비를 초래할 수 있다. 또 다른 문제점으로 인증서를 수신하고, 확인하고, 검증하는 단계가 각 노드마다 이루어 져야하므로 각 노드의 오버헤드overhead 또한 증가하게 되는 문제점이 발생한다. 그래서 본 알고리즘은 목적지를 노드를 찾고자 할 때는 중간 노드들의 인증서를 추가하지 않고, 효과적인 플러딩 방법들을 통해 목적지 노드만을 찾는 과정을 거친다. 이 과정을 통해 출발지에서 목적지까지의 경로 노드수는 현저하게 줄어들게 되며,그림 4와 같이 목적지, E 까지의 최단 경로(A→B→C→D→E)를 찾는다.

두 번째 단계는, 찾아진 목적지 노드가 신뢰할 수 있는 지를 판단하는 단계다. 이 단계에서 목적지 노드의 공개키가 포함된 인증서를 출발지 노드로 중간 노드들을 통해서 보내게 된다. 그림 4에서 보면, 먼저 A는 E의 신뢰할 수 있는 공개키를 얻기 위해 E의 인증서를 받아야 되는데, E의 인증서를 신뢰하는 노드는 E와 1홉 떨어져 있고 E의 인증서를 발행한 노드 'D'다. 그리고 D의 인증서를 신뢰하는 노드는 C이며 C를 신뢰하는 노드는 B, B를 신뢰하는 노드는 A가 된다. 이러한 관계를 이용해 노드 E는 앞 단계에서 찾아진 최적의 경로(E→D→C→B→A)로 출발지A를 향해 CRREP 패킷을 보내는 데, 이 때 그 경로상의 각 노드는 자신의 인증서를 CRREP 패킷에 추가하여 출발지까지 전송한다. 이렇게 전송 받은 인증서를 인증서 체인의 신뢰 관계를 이용해 그림-5와 같이 E를 신뢰하는 D, D를 신뢰하는 C, C를 신뢰하는 B, 그리고 B를 신뢰하는 A의 신뢰관계를 통해, A는 E의 인증서에서 신뢰할 수 있는 Destination 노드, E의 공개키를 얻을 수 있게 된다.

A<<B>> B<<C>> C<<D>> D<<E>>

그림 5. 출발지 A가 목적지 E의 신뢰할 수 있는 인증서 획득 과정

마지막 단계는 목적지 노드가 출발지 노드를 신뢰하는 단계이다. 목적지, E의 신뢰할 수 있는 공개키를 획득한 A는, 다시 자신의 인증서를 목적지 도메인, E로 보내고 경로상의 다른 노드들도 인증서를 추가하여 E로 하여금 A의 인증서가 신뢰할 수 있도록 그림-6의 과정을 지나게 된다.

E<<D>> D<<C>> C<<B>> B<<A>>

그림 6. 목적지 E가 출발지 A의 신뢰할 수 있는 인증서 획득 과정

이러한 3단계의 핸드쉐이크(handshake) 과정을 거치면 출발지와 목적지 노드는 서로를 신뢰하게 되고 안정하게 통신할 수 있는 준비가 된다.

3. 결론 및 향후 과제

본 논문에서는 MANETs에서 각 노드들이 안전하고 효과적으로 통신하기 위해 효율적인 flooding 방법을 이용하여 신뢰할 수 있는 최적의 경로를 탐색하기 위한 구조를 연구하였다.

MANETs 환경은 모든 노드들이 계층적이지 않으므로, 경로를 탐색하는 라우팅 방식이 인증서 체인들 속에서 신뢰관계에 기반하여 안전하게 통신을 하고자 하는 두 노드간의 경로 탐색 과정과 일치함을 발견하고, 효과적인 경로탐색 과정을 Ad hoc network의 인증서 체인의 탐색과정에 최초로 적용해 보았다.

단순한 flooding 방식은 출발지에서 경로를 찾기 위해 전달한 패킷이 노드의 전송 범위가 멀어 질수록 모든 노드의 수만큼 증가하는데 반해 DP, TDP등의 개선된 플러딩 방식을 적용하면 각 노드가 재 전송해야하는 수와 한 노드가 받는 패킷의 수가 급격히 줄어드는 것을 알 수 있다.

그러므로 많은 노드들이 불필요하게 시스템의 모든 노드들에게 자신의 인증서를 전송할 필요 없이 최소의 전달만으로 신뢰관계를 형성할 수 있게 되어 시스템이 보다 안전한 상태에서 신뢰관계를 형성할 수 있게 된다. 앞으로 이렇게 형성된 시스템이 보다 안전하게 유지되도록 인증서 취소 목록의 적절한 관리를 위한 연구와 비용적인 측면에서 시스템의 성능과 안정성이 균형을 이루기 위한 연구가 이루어져야 한다.

참 고 문 헌

[1] Srdjan Capkun, Levente Buttyán and Jean-Pierre Hubaux, "Self-Organized Public-key Management for Mobile Ad Hoc networks",*IEEE transactions on mobile computing* vol.2, no.1, January 2003.

[2] C.E. Perkins, "Ad Hoc On-Demand Distance Vector (AODV) Routing", Internet Draft, *IETF MANET Working Group*, draft-ietf-manet-aodv-12.txt, November 2002.

[3] Williams, B. and Camp, T,"Comparison of broadcasting techniques for mobile ad hoc networks", *In Proceedings of the ACM International Symposium on Mobile Ad Hoc networking and Computing (MOBIHOC)*, pp.194-205. 2002.

[4] H. Lim and C. Kim, "Flooding in Wireless Ad Hoc networks", *Computer Comm.*J vol.24, no.3-4, pp.353-363, 2001.

[5] W. Lou and J. Wu, "On reducing broadcast redundancy in ad hoc wireless networks," *IEEE Transactions on Mobile Computing*, vol.1, no.2, Apr 2002.