모바일 애드혹 네트워크의 안전하고 효과적인 최적의 인증경로 탐색 기법

(A Secure and Effective Optimal Path Searching Method on Certificate Chains in Mobile Ad hoc NETworks)

최 성 재 † 김 용 우 † 이 홍 기 †† 송 주 석 ††† 양 대 헌 ††††
(SungJae Choi) (YongWoo Kim) (HongKi Lee) (JooSeok Song) (DaeHun Nyang)

요 약 모바일 애드혹 네트워크는 기존의 시스템처럼 인증기관(Certificate Authority)이나 중앙 집중화된 서버를 통해 노드들에 대한 신뢰와 온라인 접근을 제공하지 않는다. 그러나, 시스템의 노드들은 서로 안전하게 데이타를 주고받기 위해서 경로를 탐색하는 것뿐만 아니라, 서로를 신뢰할 수 있게 하는 과정이 반드시 필요하다. 이러한 이유 때문에 온라인 신뢰기관이나 인증 저장 공간을 요구했던 전통적인 보안 구조는 안전한 애드혹 네트워크에는 적합하지 않다. 이에 본 논문에서는 애드혹 네트워크 환경에서 효과적인 플러딩(flooding) 기법을 사용하여 노드 사이에 '안전하고 효과적인 최적의 인증경로탐색기법'을 제안한다. 이 시스템은 브로드캐스팅(broadcasting)을 통해 목적지만을 찾는 일반적인 라우팅 프로토콜만을 의미하는 것이 아니라, 통신하고자 하는 노드를 안전하고 효과적으로 탐색하며, 찾아진 경로 또한 그 경로에 있는 노드간의 신뢰를 통해 검증하는 과정을 포함한다.

키워드 : 애드혹 네트워크, 플러딩, 보안, 인증서

Abstract In opposition to conventional networks, mobile ad hoc networks usually do not offer trust about nodes or online access through certificate authorities or centralized servers. But, nodes in those systems need process that can search path as well as trust each other to exchange data in safety. For these reasons, traditional security measures that require online trusted authorities or certificate storages are not well-suited for securing ad hoc networks. In this paper, I propose a secure and effective method to search the optimized path using profitable flooding techniques on certificate chains in MANETs(Mobile Ad hoc NETworks). This system includes not only using routing protocols that are generally broadcasting packets but also finding nodes securely and verifing the process through trust relationships between nodes that are searched.

Key words : Ad hoc network, flooding, security, certificate

1. 서 론

기지국이나 Access Point(AP)등 어떤 기존 네트워크 인프라도 갖지 않는 애드혹 네트워크 환경의 노드들은 자유로이 이동할 수 있고, 동적으로도 연결되어질 수 있다. 또한 애드혹 네트워크에서 모든 노드의 통신이 중앙의 AP를 거치지 않고 단순히 다른 노드들과의 연결 과정을 통해 여러 홉을 경유하여 'End-to-End' 데이타 전송이 수행된다. 그리고 최소의 종단간 지연시간으로 데이타를 목적지 노드까지 전송하기 위해 어떤 노드들을 경유하고, 또 어떤 노드들을 경유하지 않을 것인가는 매우 중요한 문제가 된다.

한편, 애드혹 네트워크의 보안(Security) 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[1]. 그러나 이러한 보안 목표를 달성하기 위해 현재까지 진행된 보안 관련 연구 중에는 노드들 간의 신뢰관계를 보안측면에서 가장 안정적으로 찾아내고, 이를 효과적으로 유지하

† 학생회원 : 연세대학교 컴퓨터과학과
ntchoi@emerald.yonsei.ac.kr
likeapro@yonsei.ac.kr
†† 비 회 원 : 연세대학교 컴퓨터과학과
lhk@emerald.yonsei.ac.kr
††† 종신회원 : 연세대학교 컴퓨터과학과 교수
jssong@emerald.yonsei.ac.kr
†††† 정 회 원 : 인하대학교 정보통신대학원 교수
nyang@inha.ac.kr
논문접수 : 2004년 9월 18일
심사완료 : 2005년 2월 4일

고자 하는 연구가 없었다. 이에, 본 논문은 각 노드들 간의 신뢰 관계에서 형성된 인증서 체인[2]에서, 애드혹 네트워크 환경에서의 라우팅 프로토콜 방식이, 새로이 신뢰 관계를 형성하고자 하는 목적을 갖고 있는 노드가 다른 노드를 찾고자 하는 탐색 과정과 유사함을 발견하였다. 즉, 애드혹 환경에서 각 노드가 다른 노드를 찾아가는 방식을 단순히 목적 노드만을 찾는 것이 아닌, 보안측면에서 안정적인 방식으로 신뢰할 수 있는 노드를 효과적으로 찾고 찾아진 경로를 검증하는 방식에 응용하였으며, 이렇게 찾아진 노드들은 서로가 신뢰를 바탕으로 통신할 수 있는 기반이 마련되었다는 것을 의미한다.

애드혹 네트워크의 모든 노드는 1홉 떨어진 인접 노드들의 정보를 알고 있다. 그래서 보안적인 측면에서 다음과 같은 가정은 가능하다. 애드혹 네트워크의 각 노드가 인접 노드들과 정기적인 폴링과정을 통해 인증서 교환이 이루어져 서로를 신뢰할 수 있는 관계가 형성되어 질 수 있다고 하자. 이렇게 모든 노드들이 그들로부터 1홉 떨어진 모든 노드들과 신뢰할 수 있는 관계가 형성되어 있다면, 한 노드가 그 인접 노드들을 신뢰하고 또 그 인접 노드는 그의 인접 노드들을 신뢰하는 과정을 통해 여러 경로의 신뢰관계로 맺어진 체인이 형성될 수 있는 데 이렇게 형성된 여러 경로들 중에서 최적의 인증서 체인의 경로를 찾는 방법은, 애드혹 네트워크에서 라우팅 경로를 찾는 방식과 유사하다고 할 수 있다.

애드혹 네트워크의 라우팅 방식 중 프로엑티브(proactive) 방식으로 경로를 찾는 경우 주기적인 라우팅 정보를 브로드캐스팅 함으로 인해 무선 대역폭의 낭비가 크며, 빈번한 이동성을 갖는 애드혹 특성 때문에 라우팅 패킷의 부하가 증대되는데, 특히 노드 수가 많아질수록 이 부하의 정도는 더 심각하다. 이러한 프로엑티브 방식의 문제점들로 인해 본 논문에선 경로를 찾는 방법을 리엑티브(reactive) 방식의 대표적 방법의 하나인 Ad hoc On-Demand Distance Vector Routing(AODV) 방식을 이용하여, 출발지에서 안전한 통신을 하고자 하는 목적지까지의 신뢰관계를 찾아보았다. 그러나 물론, 이 AODV 방식도 여러 가지 문제가 있는데 대표적인 문제가 플러딩이다. 기존의 프로엑티브 방식에서 일어나는 플러딩의 가장 중요한 문제는 비용 및 효율성의 측면과 불필요한 대역폭의 낭비에서 많은 문제점이 있어 기본적으로는 AODV가 목적지 노드들 찾아가는 방법을 이용하되 플러딩 방식에 있어서는 수정된 방식[3,4]을 사용하고자 한다. 이러한 방식의 기본적인 생각은 Williams, B.와 Camp, T가 분류한 4개의 프로토콜 그룹[5] 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 되어, 무조건 브로드캐스팅 하는 전통적 플러딩 방식보다는 효과적으로 경로를 찾을 수 있는 방법이다. 특히 이 방법들 중 Dominant-pruning(DP), Total Dominantpruning(TDP) 플러딩 방식을 적용하여 애드혹 환경에서의 인증서 체인을 찾기 위한 패킷 플러딩의 효율성을 높였다. 이런 과정을 거쳐 검색된 경로는 시스템의 노드들에 의해 발행되고, 유지되는 인증서를 통해서 서로를 신뢰하는 과정을 거치며, 완전히 검증된 경로로만 통신하므로 보안측면에서 안전하다고 하겠다.

본 논문의 구성은 다음과 같다. 2장에서는 MANETs에서 현존하는 라우팅 방식, 보안측면에서의 연구 그리고 효과적인 플러딩에 관련된 문제들을 살펴보고, 3장에서는 최적의 인증서 체인을 찾기 위한 구조를 제안한다. 4장은 시뮬레이션 결과를 보여주고, 5장에서 결론을 맺는다.

2. 관련연구

현재까지 애드혹 네트워크에서 가장 많이 연구되고 있는 분야는 라우팅 프로토콜 분야로, 라우팅 프로토콜은 일반적으로 프로엑티브 방식과 리엑티브 방식으로 분류되고 있다. 애드혹 네트워크의 라우팅 프로토콜에 대한 연구에 덧붙여 현재, 패킷의 재 전송 횟수를 줄여 주변 노드로 브로드캐스팅 하는 기술의 효율성을 높이자는 연구들도 진행되고 있다[3,4,6,7].

특히, Self-pruning(SP)의 경우, 각 노드는 이웃 노드들에 대한 정보를 갖고 있고, 정기적으로 헬로우 패킷을 통해 인접 노드들의 리스트를 교환한다. 패킷을 받고 이를 다시 전송하고자 하는 노드는 수신단의 인접 리스트와 송신단의 인접 리스트의 비교를 통해 수신된 패킷을 전송할 것인지 하지 않을 것인지를 결정한다. SP의 경우[3] 패킷을 전송하는 노드, u는 전송 패킷에 자신의 인접 노드 list, N(u)를 더하여 전송을 하며, 이 패킷을 수신한 노드, v는 자신이 재 전송할 노드의 리스트, S를 S=[N(v)-N(u)-{v}]로서 결정하여 재 전송 횟수를 줄이는 방법이다. 이러한 방법과 유사한 연구로는 W.Peng과 X.Lu의 Scalable Broadcast Algorithm(SBA)[7]도 있다.

DP[3]방법은 확장된 인접 노드 정보를 사용하는데 이는 SP 방법이 바로 인접한 노드들에 대한 정보만을 이용하는데 반해, 이 방법은 2홉 이내에 도달 가능한 노드들에 대한 정보를 이용한다. 다시 말해, 이 방법은 각각의 노드가 자신의 바로 1홉 떨어진 노드들의 정보가 변

경될 때 마다 그것을 인접 노드들에게 알려 주어서 모든 노드가 1홉이 아닌 2홉 떨어진 노드들에 대한 정보를 갖게 되어 플러딩 되는 패킷의 수를 줄일 수 있다. 예를 들어, 노드 u의 2홉 이내의 리스트를 N(N(u))라고 하면, 노드 v의 포워드 리스트(forward list), F는 U=N(N(v))-N(u)-N(v) 에 포함된 모든 노드가 패킷을 받도록 하면 된다. 또한 N(N(u))의 노드는 u가 패킷을 보낼 때 받게 되므로 [B(u,v)=N(v)-N(u)]에 속하는 노드들 중에서 포워드 리스트를 결정하면 된다. B(u,v)={b1, b2, b3,..., bn}이라고 할 때, $\bigcup_{b\in F}$ (N(b)∩U) =U 가 되도록 F⊆B(u,v)를 결정하면 된다. 그러나 이 방법은 자신의 인접 노드에 대한 정보를 교환해야 하므로 이동하는 노드들의 이동 정도가 큰 경우는 부하가 증대되어 오히려 SP 방식이 더 적당하다. 다시 말해, 이동 정도가 작아서 플러딩이 자주 일어나지 않는 경우는 DP가 적당하고 그렇지 않은 경우는 SP 방법이 적당하다.

마지막으로 TDP[4]의 경우는 DP이론에서 U의 크기를 좀 더 줄이는 이론으로 DP의 U 대신에 UTDP = N(N(v))-N(N(u))를 사용하고, B=N(v)-N(u)를 사용하여 전송할 리스트들의 크기를 줄였다. 특히 이 방법에서는 2홉 떨어진 노드들의 정보 중에서 중복되는 일부의 노드들을 조금 더 제거해서 효율을 높인 TDP와 partial dominant pruning(PDP) 알고리즘을 제안했다.

한편, 현재까지 애드혹 네트워크에서 이용되는 정보의 보안을 위해서 제안된 구조는 많지 않다. 그 이유는 다른 무선 네트워크가 일부의 구조를 갖는 반면 애드혹 네트워크는 어떤 기반구조도 갖지 않기 때문에 연구에 많은 제한이 있으며, 공개키를 이용한 방식의 경우는 더욱 제한적이다.

공개키를 이용한 보안구조는 먼저, Zhou와 Hass가 애드혹 네트워크의 보안 목표를 정의하고, 키 운영 서비스를 제공하기 위해 threshold cryptography 사용한 분산된 공개키 운영 구조를 제안했다[1]. 그 이후, [8]에서도 threshold cryptography에 기초한 접근을 보이는데 특히 이 논문에서는 노드들의 개인키 분배 능력을 공평하게 해서 부하를 줄이고 가용성을 증대시키는 구조를 제안했다. 그러나 이들 연구들의 공통적인 문제점은 시스템 초기단계에 어떤 신뢰기관에 의해 '임계값(t : threshold)+1' 노드들이 반드시 초기화되어야 한다고 가정하는 것이다. 순수한 의미의 어떤 기반구조도 없는 보안 구조로는 먼저, 라우팅 목적을 수행하기 위해 계층구조를 이용하여 제안된 "End-to-End data authentication scheme"이 있는데. 이 논문에서 저자는 인증 구조를 위해 TCP와 IP 의 계층적 구조를 이용하였다[9]. 또 다른 구조는 [2]를 들 수 있는데, 이 구조 또한 어떤 중앙 집중적인 기반구조도 없이, 각 노드들로 하여금 스스로 공개키·개인키 쌍을 만들고, 인증서도 발행할 수 있는 구조를 제안하고 있다.

3. 효율적인 인증경로 탐색과정

본 논문의 목적은 애드혹 환경에서, 노드간의 인증서 체인을 안정적이고, 효과적으로 찾기 위한 것인데, 제안하는 모델의 기본적 운영을 위해 다음과 같은 가정을 한다. 먼저 애드혹 환경의 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[2])이 아닌, 자신으로부터 1홉 이내의 노드들 사이로 제한하고자 한다. 신뢰 관계가 형성된 각각의 노드들은 그들 간에 인증서를 발급하는 과정을 통해 시스템의 인증서 체인을 형성한다. 이렇게 형성된 환경에서 플러딩을 통해 인증서 체인을 찾고, 찾아진 경로를 이용해 출발지(source)와 목적지(destination)간의 신뢰관계를 형성하여 안전하게 통신할 수 있는 여건을 조성하고자 하는 것이 본 제안의 목적이다. 이를 위해 시스템 초기 설정 과정을 먼저 설명하고, Certificate-chain Routing REQuest(CRREQ) 송신과 Certificate-chain Routing REPly(CRREP) 수신과정을 통해 최적의 인증서 체인을 찾고자 한다. 각 단계의 상세한 내용은 아래에서 설명한다.

3.1 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 1홉 떨어져 있으며, 안전한 채널을 갖고 있는 A와 B는 서로의 인증서를 각각 발행한다. 즉, A는 B의 인증서, 「A<<B>>」를 발행하고 B도 A의 인증서, 「B<<A>>」를 발행한다.

이렇게 발행된 인증서에는 상대방의 정보(예, 상대방의 공개키, 상대의 이름, 유효 기간등)가 발행자의 개인

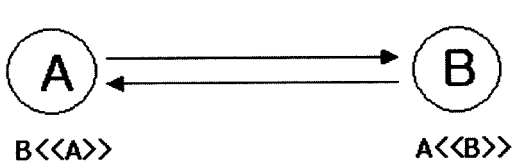

그림 1 인증서 발행

키를 이용해 해쉬된 서명을 포함하여 신뢰할 수 있는 정보가 된다. 이러한 발행 과정은 시스템의 모든 노드들이 인접 노드들에 대한 인증서의 발행이 끝나는 시점까지 이루어진다. 이러한 발행 과정이 끝나면 전체 시스템은 정상적으로 동작할 준비가 된다.

인증서의 발행이 끝나게 되면, 두 번째 단계로는 발행된 인증서의 교환이 이루어진다. 이 단계에서 각각의 노드는 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 애드혹 네트워크의 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 통신경로 탐색에 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.

3.2 최적의 인증경로 탐색

먼저, 출발지 노드는 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 해야 할 일은 통신하고자 하는 목적지를 향해서 CRREQ Packet을 브로드 캐스팅 하는 것이다. 출발지 노드에서 이 패킷을 브로드 캐스팅 할 때는 일단 자신이 원하는 목적지 노드에 대한 정보를 패킷에 실어 단순히 이웃 노드들에게 전송하면 된다.

3.2.1 CRREQ 수신

출발지로부터 전송된 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 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.

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

이러한 과정들을 통해 목적지 노드가 CRREQ 패킷을 받으면 그 안에서 목적지 노드는 출발지 노드의 인증서

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

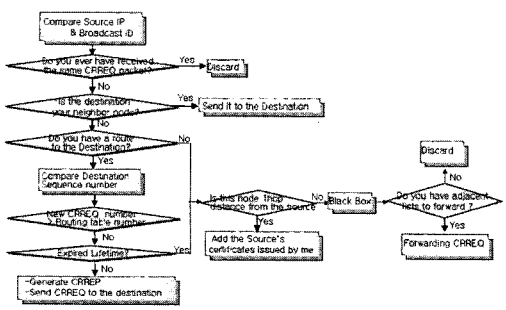

그림 3 CRREQ 전달 절차에 대한 순서도

와 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.

3.2.2 CRREP 송신

출발지에서 전송한 CRREQ 패킷이 목적지에 도착하면, 목적지 노드는 CRREP패킷을 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 일련번호에 1을 증가시킨 값을 CRREP 패킷의 Destination Sequence Number에 저장하고 이를 축적된 경로정보를 참조로 CRREQ를 발생시켰던 노드 방향으로 유니캐스트(unicast) 한다.

이때 이 패킷을 전송하는 목적지 노드의 인증서를 패킷에 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 여러 노드들의 경우에서 살펴보면 그림 5와 같다.

그림 5에서처럼, 출발지, A와 목적지, O가 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 오버헤드 또한 증가하게 되는 문제점이 발생한다. 그래서 제안하는 알고리즘에서는 목적지 노드를 찾고자 할 때는 중간 노드들의 인증서를 추가하지 않고, 효과적인 플러딩 방법들을 통해 목적지 노드만을 찾는 과정을 거친다. 이 과정을 통해 출발지에서 목적지까지의 경로 노드의 수는 현저하게 줄어들게 되며, 그림 5와 같이 O까지의 최단

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

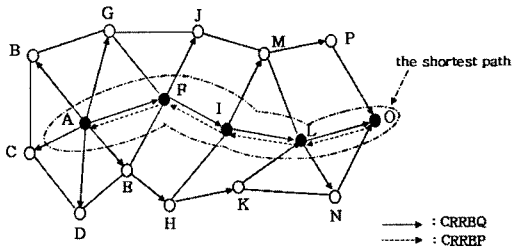

그림 5 CRREP 패킷의 전송

경로(A→F→I→L→O)를 찾는다.

두 번째 단계는, 찾아진 목적지 노드가 신뢰할 수 있는 지를 판단하는 단계다. 이 단계에서 목적지 노드의 공개키가 포함된 인증서를 중간 노드들을 통해서 출발지 노드로 보내게 된다. 그림 5에서 보면, 먼저 A는 O의 신뢰할 수 있는 공개키를 얻기 위해 O의 인증서를 받아야 되는데, O의 인증서를 신뢰하는 노드는 O와 1홉 떨어져 있고 O의 인증서를 발행한 노드 L이다. 그리고 L의 인증서를 신뢰하는 노드는 I이며 I를 신뢰하는 노드는 F, F를 신뢰하는 노드는 A가 된다. 이러한 관계를 이용해 노드 O는 앞 단계에서 찾아진 최적의 경로(O→L→I→F→A)로 A를 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 6과 같이 O를 신뢰하는 L, L을 신뢰하는 I, I를 신뢰하는 F, 그리고 F를 신뢰하는 A의 신뢰관계를 통해, A는 O의 인증서에서 신뢰할 수 있는 노드 O의 공개키를 얻을 수 있다.

마지막 단계는 목적지 노드가 출발지 노드를 신뢰하

A<<F>> F<<I>> I<<L>> L<<O>>

그림 6 출발지 A가 목적지 E의 신뢰할 수 있는 인증서 획득 과정

는 단계이다. O의 신뢰할 수 있는 공개키를 획득한 A는 다시 자신의 인증서를 O로 보내고 경로상의 다른 노드들도 인증서를 추가하여 O로 하여금 A의 인증서가 신뢰할 수 있도록 그림 7의 과정을 지나게 된다. 이러한 3단계의 핸드쉐이크(handshake)과정을 거치면 출발지와 목적지 노드는 서로를 신뢰하게 되고 안정하게 통신할 수 있는 준비가 된다.

O<<L>> L<<I>> I<<F>> F<<A>>

그림 7 목적지 O가 출발지 A의 신뢰할 수 있는 인증서 획득 과정

4. 시뮬레이션 결과 및 분석

본 논문에서 제안한 모바일 애드혹 환경에서 최적의 인증서 체인상의 경로를 찾는 방법의 효율성을 검증하기위해 시뮬레이션을 수행하였다. 기존에 인증서를 통해 노드 사이의 신뢰관계를 형성하는 과정을 효과성 측면에서 분석한 연구가 없었기 때문에 그러한 방법과의 효과성 비교는 할 수 없었다.

대신 본 논문에서는, 인증서 체인 탐색의 성능 평가를 위해 크게 두 가지로 비교대상을 선택하였는데, 하나는 '단순한 플러딩' 또는 '블라인드 플러딩(Blind Flooding, B.F)'이라고 불리는 '일반적인 브로드 캐스팅' 방법과 다른 하나는 '개선된 플러딩', DP와 TDP 방법이다. 일반적으로 브로드캐스팅을 통한 전송방식에 인증서를 추가하여 서로 신뢰할 수 있는 노드를 찾는 과정과 효율성이 입증된 효과적인 플러딩 방법들을 통한 신뢰할 수 있는 노드의 탐색 방법과의 비교를 통해 제안하는 알고리즘의 효과성을 증명하였다.

여기서 비교 대상들은 단말의 전송거리 거리(Tr)의 변화를 통해 네트워크내의 각 노드들이 평균적으로 수신한 패킷의 크기와 전송해야 하는 노드의 수를 측정함으로써 성능을 비교하였다. 평균적으로 수신한 패킷크기가 증가할수록, 각 노드가 처리해야할 데이타의 크기는 늘어나게 되고, 오버헤드도 증가하게 되며 자원의 소모도 많아지게 된다. 또한 신뢰관계를 형성하기 위한 인증서의 검증과정에서도 더욱 많은 시간이 소요되므로, 평균 수신한 패킷 크기를 측정대상으로 하는 것은 필수적 검증요소이다. 그리고 각 노드가 재 전송해야 하는 노드수도 제한된 자원으로 보다 높은 효율을 내기 위해선 보다 적은 노드에게로만 패킷을 재 전송해야 하므로 이 재 전송해야 하는 노드 수 또한 검증을 위한 중요한 파라미터이다. 물론, 인증서를 사용한 시스템과 그렇지 않은 시스템과의 비교도 할 수 있으나 전송거리에 따른 패킷의 크기의 변화의 경우 인증서의 크기에 비례하여 패킷의 크기가 증가되고, 재 전송해야 하는 노드의 경우는 인증서를 사용한 경우와 그렇지 않은 경우와 동일한 결과를 가져오므로 이의 비교는 의미가 크지 않아 생략하였다.

효과적인 성능 비교를 위해 본 논문에서는 가장 이상적인 MAC 계층을 가정하여 어떤 정체현상(congestion)이나 충돌(collision)은 일어나지 않는 것으로 하였다. 시뮬레이션을 위해 본 논문에서 사용한 주요한 파라미터는 표 1과 같다.

표 1 시뮬레이션 파라미터

Simulation Parameter	Value
Simulator	NS-II
네트워크 size	100×100m2
통신 반경	25~70
단말의 수	40~80
패킷 크기	512byte
Simulation time	120sec
시도 횟수	10

그림 8은 노드의 수를 40개로 고정해 놓고, 네트워크의 크기를 100×100(m^2)로 설정한 후, 전송 범위를 늘려가면서 BF, DP 그리고 TDP 방법을 사용하여 시스템의 노드들이 수신한 CRREQ 패킷의 크기를 분석한 그래프이다. 그래프에서 X축은 전송 범위(Transmitter Range)를 나타내며, Y축은 거리의 증가에 따른 각각의 노드가 수신한 패킷의 크기를 나타낸다.

전송범위 값이 작을 때는 노드들이 많이 연결되어 있지 않아서 각 노드가 수신한 패킷의 크기가 작음을 알 수 있다. 그러나 전송 범위가 증가할수록 각 노드가 받는 패킷에 주변 노드들의 신뢰정보들이 추가되어 패킷 크기는 점점 증가하게 된다. B.F 방법에서 거리가 증가함에 따라 출발지와 목적지 노드사이에 존재하는 노드

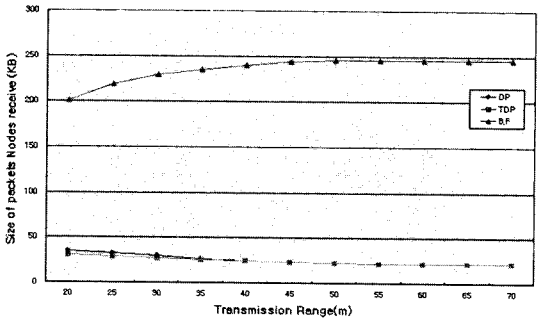

그림 8 노드가 40인 네트워크에서 노드가 수신한 패킷의 크기

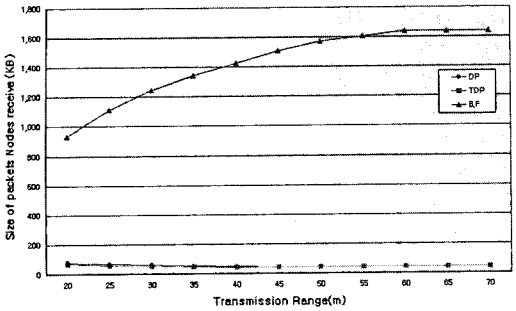

그림 9 노드가 80인 네트워크에서 노드가 수신한 패킷의 크기

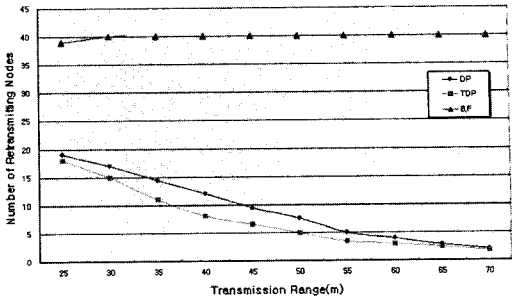

그림 10 노드가 40인 네트워크에서 재 전송해야 하는 노드의 수

수도 증가하여, 거리가 증가할수록 중간에 있는 노드가 수신해야하는 패킷의 크기도 증가한다. 이는 인접 노드들을 신뢰하기위해 각 노드들이 패킷에 저장해야 하는 주변 노드들에 대한 인증서를 포함한 정보들의 증가를 의미한다. 그러나, DP와 TDP는 서서히 감소하다가 노드수에 해당하는 패킷의 크기에 거의 근접하는 양상을 보이며 거리가 전송거리가 40m를 넘어서는 DP와 TDP가 거의 동일한 결과를 보인다.

그림 9는 80개의 노드의 수를 갖는 네트워크에서 전송 거리의 변화에 따라 노드가 수신한 CRREQ 패킷의 크기를 분석한 그래프인데 노드가 40개 있을 때보다 인증서 체인을 찾기 위해 노드가 수신한 패킷의 크기가 더 증가함을 보여주며, 여기서도 DP와 TDP가 B.F에 비해 더 좋은 성능을 보인다.

그림 10은 노드의 수를 40개로 고정해 놓고, 전송 범위를 늘려가면서 3가지의 플러딩 방법을 사용하여 CRREQ 패킷을 재 전송해야 하는 노드의 수를 측정한 결과를 분석한 그래프다. 그래프에서 X축은 전송 범위를 나타내며, Y축은 재 전송해야 하는 노드의 수를 나타낸다.

전송 거리의 값이 작을 때는 노드들이 많이 연결되어 있지 않아서 전체 노드의 수인 40개 보다 재 전송해야 하는 노드의 수가 작음을 알 수 있다. 그러나, 점차 전송거리가 증가함에 따라 B.F을 사용했을 때는 그래프의 맨 위에서처럼 네트워크의 모든 노드들이 전부 CRREQ 패킷을 재 전송해서 인증서 체인을 탐색해야 하지만, DP, TDP를 사용하게 되면 인증서 체인을 탐색하기 위해 패킷을 재 전송해야 하는 수는 두 알고리즘에 의해 현저히 줄어드는 것을 알 수 있다. 다시 말해 불필요하게 재 전송해야 하는 노드수가 줄어들어, 결국 출발지에서 목적지까지 향하는 노드들이 인접 노드들을 신뢰하거나 경로를 찾고 유지하는데 많은 자원을 소모하지 않고도 안정적인 관계를 형성할 수 있음을 알 수 있다.

그림 11은 노드의 수를 80개로 증가시켰을 때 Tr를

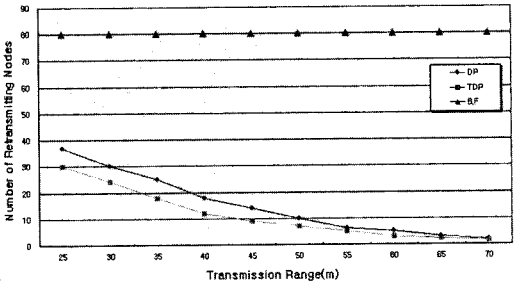

그림 11 노드가 80인 네트워크에서 재 전송해야 하는 노드의 수

늘려가면서 재 전송해야 하는 노드들의 수를 측정한 그래프이다. 이 경우에서도 앞의 경우에서 보는 것처럼 DP와 TDP 방법은 B.F에 의한 방법보다 CRREQ 패킷을 재 전송해야 하는 수치가 크게 줄어든다.

5. 결론 및 향후 과제

본 논문에서는 모바일 애드혹 네트워크에서 각 노드들이 안전하고 효과적으로 통신하기 위해 효율적인 플러딩 방법을 이용하여 신뢰할 수 있는 인증서 체인상의 경로를 탐색하고 검증하는 구조를 제안하였다.

애드혹 환경은 모든 노드들이 계층적이지 않으므로, 경로를 탐색하는 라우팅 방식이 시스템의 노드들 사이의 인증서 체인 속에서 신뢰관계에 기초하여 안전하게 통신을 하고자 하는 두 노드간의 경로 탐색과정과 일치함을 발견하였고, 효과적인 경로탐색 과정을 애드혹 네트워크 인증서 체인의 탐색과정에 최초로 적용해 보았다. 단순히 브로드캐스팅하는 플러딩 방식은 출발지에서 경로를 찾기 위해 전달한 패킷이 노드의 전송 범위가 멀어 질수록 모든 노드의 수만큼 증가하는데 반해 DP, TDP등의 개선된 플러딩 방식을 적용하면 각 각의 노드가 재 전송해야하는 수와 한 노드가 받는 패킷의 수가 급격히 줄어들게 됨을 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] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Nework Megazine*, vol.13, no.6, Dec 1999.

[2] S. Capkun, L. Buttyán and J. Hubaux, "SelfOrganized Public-key Management for Mobile Ad Hoc networks," *IEEE transactions on mobile computing* vol.2, no.1, Jan 2003.

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

[4] 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.

[5] B. Williams, and T. Camp, "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.

[6] S. Tseng, Y. Chen and J. Sheu, "The broadcast storm problem in a mobile ad hoc network," *In Proceedings of the ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile System*(MSWIM), 2000.

[7] W. Peng and X. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," *In Proceedings of MOBIHOC*, 2000.

[8] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc networks," *IEEE ICNP '2001*, 2001.

[9] L. Venkatraman and D. Agrawal, "A Novel Authentication scheme for Ad hoc networks", *IEEE 2000*, Nov 2002.

최 성 재

1996년 2월 육군사관학교 전자공학과 학사. 2005년 2월 연세대학교 컴퓨터 과학과 석사. 관심분야는 Mobile network, Information Security, Ad hoc network

김 용 우

2001년 2월 연세대학교 전기·전자공학과 학사. 2001년 1월~2003년 7월 삼성전기 중앙연구소 S/W연구팀 주임연구원 2003년 9월~현재 연세대학교 컴퓨터 과학과 석사. 관심분야는 네트워크 보안, Mobile IPv4/6, MANET 통신

이 홍 기

1993년 2월 육군사관학교 졸업. 2000년 2월 연세대학교 컴퓨터 과학과 석사 2004년 3월~현재 연세대학교 컴퓨터 과학과 박사과정. 관심분야는 네트워크 보안, RFID 보안, MANET 통신

송 주 석

1976년 2월 서울대학교 전기공학과 학사 1979년 2월 한국과학원 전기전자공학과 석사. 1988년 2월 University of California at Berkeley Ph.D. 1989년 3월~현재 연세대학교 컴퓨터과학과 교수. 관심분야는 유무선통신, 정보보호

양 대 헌

1994년 2월 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업. 1996년 2월 연세대학교 컴퓨터 과학과 석사. 2000년 8월 연세대학교 컴퓨터 과학과 박사 2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원. 2003년 2월~현재 인하대학교 정보통신대학원 전임강사. 관심분야는 암호이론, 암호프로토콜, 인증 프로토콜, 무선 인터넷 보안