안정적인 동적 복합 ad-hoc 네트워크와 이에 대한 신뢰성 있는 키 인증과 키 관리

이충세*

요 약

이 논문에서는 ad-hoc 네트워크의 제한된 문제점들을 살펴보고 ad-hoc 네트워크에 보다 효율적으로 적용할 수 있는 2-tier 계층적 네트워크를 적용하는 새로운 동적 라우팅 방법을 제안한다. 효율적으로 네트워크를 관리하기 위하여 proactive와 reactive 라우팅 방법의 장점을 결합할 수 있는데, 이라한 방법을 NSDR(New Secure Dynamic Routing)이라고 정의한다. 이 논문에서는 또한 이러한 네트워크상에서의 신뢰할 수 있는 인증방법과 키 관리 방법을 제안한다. Ad-hoc 네트워크와 차세대 모바일 네트워크와 결합하여 신뢰성을 향상시키는 인증 방법이나 키 관리를 위한 부차적인 연구를 수행하고 있다.

Trustworthy authentication and key management for NSDR ad-hoc network

Chung Sei Rhee*

ABSTRACT

In this paper, we consider the limit of the previous works for ad-hoc network, then propose a dynamic routing scheme which employs a 2-tier hierarchical structure. We adopt the advantages of proactive and reactive routing scheme for efficient network management. We define this method as NSDR(New Secure Dynamic Routing) scheme. We also propose a trustworthy authentication and key management for the proposed ad-hoc network. We currently study the possibility that ad-hoc networks can provide a service such as key management and authentication for the next generation mobile network.

Key words : ad-hoc network, dynamic routing, security, public key, private key, certification, topology

접수일(2012년 7월 10일), 수정일(1차: 2012년 9월 11일, 2차: 2012년 9월 21일), 게재확정일(2012년 9월 25일)

* 충북대학교 소프트웨어학과

1. 서 론

Ad-hoc 네트워크는 멀티-홉 패킷트 교환을 이용하여 서로 통신하는 모바일 네트워크이다. Ad-hoc 네트워크는 고정된 개념에 의존하지 않는 이동 호스트들로 구성되어 있는 고유한 특성을 가지기 때문에 여러 분야에 사용할 수 있는 장점을 가지고 있고 또한 IETF MGET WG나 Bluetooth Consortium과 같은 다양한 그룹에 의해 많은 연구가 이루어지고 있다.[2,5] 그러나 모든 네트워크 안에서의 통신에 한정된 자원을 이용하여 수행하기 때문에 효율적인 ad-hoc 네트워크 관리를 위해서는 무선 스펙트럼 보존(conservation of wireless spectrum), 전송전력의 최소화와 같은 해결해야 할 많은 제약이 있다.

Ad-hoc 네트워크는 구조상의 특성 때문에 신속하게 변화되기 때문에 최적의 라우팅 경로를 찾고 이를 관리하는 것이 매우 중요하고 또한 어려운 문제가 된다. 따라서 ad-hoc 라우팅 알고리즘은 빈번한 네트워크 구종의 변화에 신속하게 대응할 수 있어야 한다. 이러한 네트워크를 위한 모든 라우팅(routing) 프로토콜의 설계를 위해서는 두 노드 사이에 정확하고 효율적인 라우팅 경로를 설계하는 것이다. 특히, 라우팅 경로를 설계할 때에 제한된 컴퓨팅 자원에 대한 에너지 보존과 전송대역 소모량(bandwidth consumption)과 같은 상항들도 교려해야 한다. ad-hoc 네트워크는 낮은 전송대역 소모량과 높은 전송오류 그리고 전송회선의 불안정 때문에 전형적인 인터넷 라우팅 프로토콜을 직접 사용할 수 없다. 기존의 라우팅 프로토콜을 사용할 경우에 주기적인 메시지 교환으로 인한 망의 대역폭 낭비와 망의 동적인 변화에 신속하게 대응할 수 없다.

Ad-hoc 네트워크는 Flat Routed 구조와 계층적(hierarchical) 구조로 나눌 수 있다[3]. 네트워크상의 각 이동 노드들은 클러스터(cluster)라고 부르는 여러 개의 작은 그룹으로 분할된다. 계층적 구조는 구성상의 특성 때문에 이동 노드들의 관리가 쉽다는 장점을 갖지만 두 개의 다른 이동 노드간의 직접적인 경로가 없기 때문에 라우팅 경로를 확보하는데 최적이 아닐 경우가 많다. 반면에, Flat 네트워크는 시작 노드와 목적지 노드사이에 여러 개의 경로가 존재하는 장점을 가지고 있기 때문에 이러한 경로는 네트워크의 혼잡을 줄이는 효과와 최적의 경로를 구할 수 있지만 확장성(scalability)이 적다. 또한 빈번한 노드들의 위치 변화에 따르는 라우팅 테이블의 유지하는데 많은 시간과 계산 능력의 저하를 가져올 수 있다.

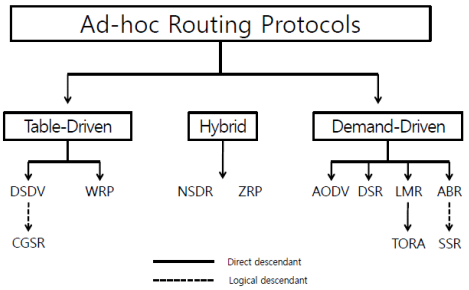
2. 관련 연구

2.1 프로토콜 라우팅

Ad-hoc 네트워크에 대한 모든 라우팅 프로토콜의 목표는 네트워크상의 임의의 두 노드들 사이에 정확하고 효율적인 라우팅 경로를 설정하는데 있다. 이러한 네트워크는 낮은 대역폭과 높은 전송 오류율 그리고 불안정한 무선 연결과 같은 특징을 갖기 때문에 전통적인 인터넷 라우팅 프로토콜을 사용하는 것이 불가능하다. 전통적인 라우팅 프로토콜을 사용할 경우에, 네트워크의 대역폭에 상당한 낭비를 초래할 뿐만 아니라 네트워크 토폴로지의 동적인 변화에 적절히 대응하는 것이 불가능하다.

Ad-hoc 네트워크의 라우팅에는 테이블-구동 방식인 proactive routing 프로토콜과 요구-구동 방식인 reactive routing 프로토콜로 나누어지는데 이 두 가지 방법은 실시간 통신에 효과적이지 못하기 때문에 두 가지 방법을 절충한 HRP(Hybrid Routing Protocol) 방법이 있다.[그림 1 참조] 최근에 이와 같은 하이브리드 방식이 이동 통신 ad-hoc 네트워크에 적합한 방법으로 고려되고 있고 대표적인 HRP 방법으로 ZRP (Zone Routing Protocol) 등이 있다. HRP 프로토콜은 테이블-구동 프로시저의 영역을 zone이라 부르는 한 노드의 이웃 노드들로 제한하여, 테이블-구동 방식과 요구-구동 방식을 단점들을 보안하기 위하여 제안되었다. 그러나 현존하는 라우팅 기법만을 이용하여 ad-hoc 네트워크에 필요한 다양한 문제에 대한 일반적인 해결 방안을 제공하지 못하고 있고, 현존하는 많은 프로토콜을 실제적으로 네트워크에 적용하는데 많은 비용이 필요하다. 또한 현재의 3세대 무선 통신망(battery powered device) 서비스와 상호 연동이 가능하게 하기 위하여 다양한 홈 네트워크나 사무실 네트워크를 위한 차세대 이동 ad-hoc 랜 환경에 전통적인

라우팅 기법을 적용하는 것이 부적절하다.



(그림1)

2.2 보안 요소

ad-hoc 네트워크에서는 빈번한 형태 변화와 함께 무선 채널을 사용하는 구조적인 특성 때문에 보안 위협에 아주 취약하기 때문에 안정적이고 효율적인 보안 극복 방안이 필수적이다. 따라서 보안은 ad-hoc 네트워크를 구성할 때, 가장 중요한 요소 중에 하나가 된다. Ad-hoc 네트워크를 위한 프로토콜을 설계할 때에 유용성, 기밀성, 무결성, 인증 그리고 부인봉쇄와 같은 보안 문제를 충분히 고려해야 한다[2].

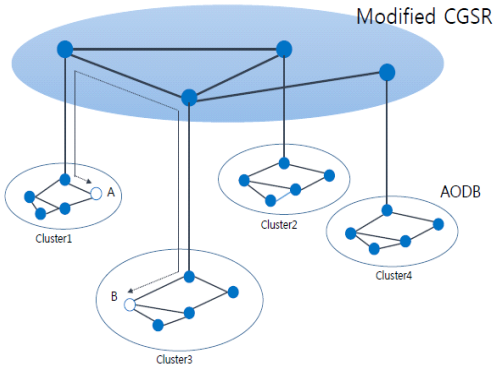
2.3 안정적인 ad-hoc 네트워크의 구현

무선 링크, 제한된 자원, 물리적 자원의 제한, 적성 지역에서의 작전 수행 그리고 빈번한 형태의 변화 때문에 ad-hoc 네트워크를 설계할 경우에 다음과 같은 사항들에 대한 충분한 대응책을 고려해야 한다.

- 무선 링크 사용에 의한 도청 (eavesdropping) 인가되지 않은 비밀 정보에 접근, 기밀성 훼손
- 네트워크에 허가되지 않은 외부인의 접근 메시지 삭제, 변조
- 변질된 이동 노드에서의 부적절한 정보 획득 및 공격
- 빈번한 네트워크 형태의 변화에 대처할 수 있는 라우팅 프로토콜

이러한 문제들을 해결하기 위하여 각 이동 노드와 각 클러스터 안에 CH와 신뢰할 수 있는 인증 메커니즘을 통하여 네트워크 외부에 있는 적의 공격이나 인가되지 않은 사용으로부터 보호하고 변질된 노드와 클러스터 헤드의 변질들을 발견하고 이들을 배제하고도 효율적인 라우팅과 안정성을 제공할 수 있는 프로토콜을 설계하는 것이 필요하다.

3. 안정된 동적 라우팅



(그림 2)

이 논문에서는 효율적인 2-tier 계층적 네트워크를 구성할 경우에 하위계층(tier-1)은 재활성(reactive) 기법[3]의 장점을 그리고 상위계층(tier-2)은 proactive 기법의 사용하는 효율적인 Ad Hoc 네트워크의 관리와 함께 경로 설정을 위한 오버헤드와 전송지연 시간을 줄일 수 있는 새로운 라우팅 기법을 제안한다. LLC 알고리즘[3]을 실행 시에 변질된 클러스터 헤드를 발견할 경우에 CH(Cluster Header)을 망에서 배제하고 하위(tier-1) 노드들 중에서 CH 역할을 대행할 수 있는 CH 재구성 알고리즘을 제시한다.

3.1 새로운 동적 하이브리드 라우팅 방법

이 논문에서 제안하는 ad-hoc 네트워크는 그림2와 같이 2개의 tier를 갖는다. Tier-1 계층에 속한 노드들 중에 최소한 하나의 노드는 상위 계층으로 연결하는 게이트웨이 역할을 하도록 지정한다. 이러한 게이트웨

이 노드들은 상위 네트워크를 설정하는데, 이러한 상위 네트워크에 계산 능력과 자원이 좋은 transmitters /receivers가 필요하다. 또한 하위 계층에 속한 노드들은 AODV[6] 알고리즘을 이용하여 On-Demand 방식으로 라우팅 경로를 설정하며, 서로 다른 하위 계층에 속한 이동 노드들 사이의 통신은 게이트웨이 역할을 수행하는 CH을 통해 전달하는데, 이때 상위 계층에 속한 노드들은 CGSR(Cluster-head Gateway Switch Routing) 프로토콜을[1, 7] 이용하여 네트워크를 만든다.

이 논문에서 제안하는 상위계층의 네트워크는 엄밀한 의미에서 순수한 CGSR이라고 볼 수는 없고, 효율적인 네트워크 관리와 채널 제어, 대역폭 할당 등을 고려하고 proactive 전략을 이용하여 변질된 클러스터 헤더를 배제하여 안전한 라우팅 루트를 설정하고 기존의 3GPP 서비스를 보다 강력한 CH와 상호 연동시킬 가능성을 고려하여 제안하였다.

3.2 CH 재-구성 알고리즘

2-tier 계층 네트워크 구조에서 각각의 CH는 하위 계층에 속해 있는 이동 노드들의 라우터 역할과 함께 세션 키를 생성하고 키 관리에 대한 책임을 다른 CH와 함께 담당한다. 따라서, 한 CH가 적에 의해 공격을 당하거나 다른 이동 노드로부터 신뢰성을 상실하였을 경우 CH를 네트워크에서 배제하고 변질된 클러스터 헤더를 대체하는 새로운 CH를 생성하여 네트워크를 재-구성해야만 한다. Chiang-Chuan Chiang 등은 LCC(Least Cluster Change) 알고리즘[7]에서 클러스터 헤더를 생성할 경우를 2가지로 제한하였으나 변질된 클러스터 헤더를 발견하는 경우 안정된 라우팅을 보장하기 위하여 LCC 방법에 (3)이 경우를 보완하여 클러스터 헤더를 재-생성한다. 클러스터 헤더를 재-생성하는 경우는 다음과 같다.

- 한 개의 클러스터 헤더가 자기의 영역을 벗어나 다른 클러스터 헤더가 있는 곳으로 이동한 경우
- 한 개의 이동 노드가 클러스터 헤더가 없는 곳으로 이동한 경우
- 시스템이 클러스터 헤더가 변질된 것을 확인한 경우

4. 키 관리와 인증 전략

공개키 암호기법을 이용하여 라우팅 정보와 데이터 트래픽에 대한 정보를 보호한다. 클러스터 키는 모든 클러스터에 대하여 유일하게 존재하고 클러스터에 속하는 모든 이동 노드들에게 분배한다. 키는 CH에 의해 생성하고 시스템 공개키로 암호화한 다음 클러스터 멤버에게 분배한다. 각 이동 노드는 공개/개인키 쌍을 갖고 있으며, 키 관리를 위한 CA(Certification Authority)을 두어 키의 바인딩과 주기적 갱신을 담당한다. CA는 공개/개인키 쌍을 갖고 있으며, 공개키는 다른 모든 노드들에 분배하고 비밀키를 이용하여 인증서를 서명하여 분배한다. 어떤 이동 노드를 더 이상 신뢰할 수 없거나 네트워크 영역을 벗어나게 되면 이러한 노드의 공개키는 폐지한다.

4.1 Threshold 암호화 기법

CA는 전체 네트워크에 대한 보안을 책임지는 객체로써 외부 적의 집중적인 공격의 대상이 되므로, 하나의 CA를 사용한다고 가정하면 끈임 없는 외부 공격으로 인하여 CA가 정상적인 역할을 수행하지 못하거나 적에게 변질되어 악용될 경우 심각한 문제를 야기시킬 수 있다. CA를 이용한 서비스를 사용하는 것이 가능하지 않다면, 이동 노드들은 다른 이동 노드를 이용하여 공개키를 얻을 수 없고 다른 이동 노드들과 안전한 교신을 수행할 수 없다. 만일 CA가 적에 의해 변질되어 비밀키가 적에게 알려지면 적은 이러한 비밀키를 이용하여 거짓된 인증서를 발행할 수 있다. 이러한 문제점을 해결하기 위하여 Threshold 기법[4]을 이용하여 시스템 키 관리 서비스의 책임을 각 CH에 분할하여 분배하고, (n, t+1) Threshold Cryptography를[2] 이용하여 2-tier 계층 구조의 중요한 요소에 속하는 각 CH의 신뢰 여부를 확인하며, 클러스터 헤드가 변질된 경우 하위 계층에 속한 이동 노드들 중에서 새로운 클러스터 헤드 역할을 수행할 노드를 신속하게 재-생성하여 네트워크를 재-구성한다.

4.2 인증 전략

이 논문에서 제안한 알고리즘을 신뢰할 수 있는 인증 절차를 수행하기 위하여 세 가지 다른 경우를 고려한다.

Case-1: CH와 들어오는(incoming) 노드 사이에 상호 인증
Case-2: 노드가 옛 클러스터에서 빠져 나와 새로운 클러스터에 조인하는 경우
Case-3: 한 클러스터에 속하는 노드가 다른 클러스터에 속하는 노드와 통신을 원하는 경우

ad-hoc 네트워크에 있는 모든 노드들은 시스템의 공개키를 알고 있다고 가정한다. 모든 CH들은 시스템의 키를 관리할 책임을 공유한다. 각 CH는 각각의 키에 유일한 클러스터 키를 갖는다. 한 개의 클러스터 키는 클러스터에 속한 모든 노드들에 의해 공유된다. 이러한 키는 클러스터 헤드에 의해 생성되어 모든 클러스터 멤버에게 분배된다. 키는 시스템의 공개키에 의해 암호화되어 헤드에 의해 전달한다. 이 논문에서는 또한 세션 키가 단지 한 개의 TCP 세션에만 타당하다고 가정한다. 적에 의한 거듭된 공격에 대응하기 위하여 시간 스탬프를 암호화하여 암호화된 메시지와 함께 동료 노드에게 보낸다.

앞에서 정의한 세 가지 경우에 대하여 인증하는 알고리즘들을 다음과 같이 구현하였다.

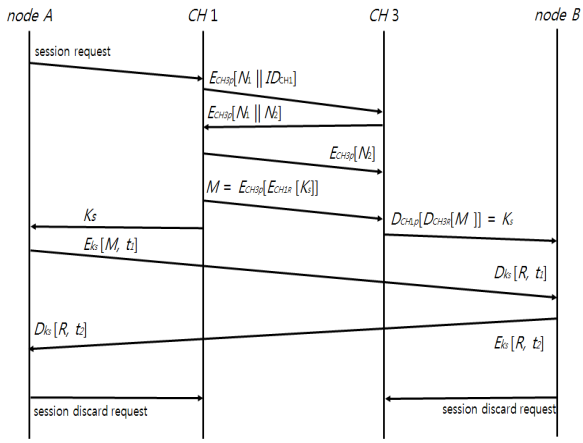
Case-1

새로운 모바일 노드가 네트워크에 처음으로 참여하면, 강력한 인증 절차가 필요하다. 이러한 인증 절차는 도전-반응(Challenge-Response)으로 이루어진다. 'Hello'라는 메시지 수단을 이용하여 노드가 CH에 메시지를 전달하면, CH는 지역적인 통신을 위하여 노드에 클러스터 키를 제공한다.

① CH는 난수 r을 생성하고 자신의 클러스터 키와 함께 도래하는 노드 A에 보낸다.
② 노드 A는 지역적인 통신을 위하여 클러스터 키를 보관한다. 노드 A는 또한 CH의 공개키를 이용하여 r을 암호화하고 이를 CH에 보낸다.
③ CH는 자신의 개인키를 이용하여 r을 해독하고 자신이 보낸 난수와 같은 값인지를 조사한다.

Case-2

노드가 자신의 클러스터를 떠나 다른 클러스터로 들어갈 경우에 새로운 CH는 이러한 노드를 자신의 클러스터에 참여하는 새로운 노드로 간주한다. 새로운 노드와 새로운 클러스터 사이의 상호 인증이 발생한다. 그런 다음, 새로운 CH는 자신의 클러스터 키를 새로운 노드에 분배한다. 종전에 노드가 속해 있던 CH는 일정한 시간 간격에 'hello' 메시지를 받지 못하면 이러한 노드를 엔트리에서 제거한다.



(그림3)

Case-3

다른 경우와 비교하여 case-3는 약간 복잡하다. 완전한 신뢰성을 갖기 위하여 세션 키를 이용하여 전체 메시지를 암호화한 다음 동료 모바일 노드에 전송한다. 공개키는 상호 인증을 위하여 사용할 수 있다. 통신에 관여하는 두 개의 노드만이 세션 키를 공유할 수 있다. 각 노드를 확실히 인증할 수 있는 알고리즘을 제안한다. 프로시저에서 통신에 참여하는 두 개의 CH는 CA 역할을 담당한다.

노드 A가 다른 클러스터에 속하는 노드 B와 통신하려면 다음과 같은 프로시저를 이용한다.

① 노드 A는 CH1에 세션 키 요청을 보낸다.
② CH1은 Noncel와 ID을 CH3의 공개키로 암호화한

다음, CH3에 보낸다.

③ CH3는 받은 메시지를 개인키를 이용하여 해독한 다음, CH1에 키를 CH3에 보냈음을 알린다.

④ CH3가 CH1을 인식하면, CH3는 CH1의 공개키로 암호화하여 답장 메시지를 보낸다. 이러한 메시지 안에는 CH3가 받은 Nonce1과 CH1에 보낸 Nonce 2를 포함시킨다.

⑤ CH1이 Nonce2을 받으면, CH3의 공개키를 이용하여 메시지를 암호화한 다음 다시 CH3에 보낸다. 이러한 프로시저가 끝나면 두 개의 CH들은 서로 신뢰할 수 있고 더 많은 통신을 위하여 안전한 세션을 개방한다.

⑥ CH1는 세션 키 K_S을 생성한 다음 두 개의 CH들로만 해독이 가능한 세션 키를 CH#에 보낸다.

⑦ CH3는 메시지 M을 해독하여 세션 키 K_S을 얻는다.

⑧ CH1과 CH3는 이러한 세션 키 K_S을 노드 A와 노드 B에 전달한다.

⑨ 노드 A는 노드 B에 세션 키로 암호화한 메시지를 보낸다. 이러한 메시지에는 메시지 M과 시간 스탬프 t_1이 포함된다.

⑩ 노드 B는 노드 A로부터 받은 메시지를 해독하고 노드 A에 암호화된 회신 메시지 R과 시간 스탬프 t_2을 보낸다.

⑪ 두 개의 노드 A와 B 사이에 비밀 메시지 교환이 이루어진 후에 각각의 노드는 두 개의 CH들에 세션 취소 요청을 한다. 요청을 받으면 CH들은 세션 키 K_S을 폐기한다.

5. 결 론

이 논문에서는 2-tier 계층적 구조를 갖는 NSDR (New Secure Dynamic Routing) 방법을 제안하였다. proactive 방법과 reactive 방법의 장점을 묶는 효율적인 라우팅 방법도 제시하였다. LCC 알고리즘에서는 한 개 또는 그 이상의 CH 재-구성이 필요한 것도 확인할 수 있다. 또한 제안한 NSDR에 대한 신뢰할 수 있는 인증 알고리즘과 키 관리 방법도 제안하였다. 이 논문에서는 또한 현재 많이 연구가 진행되고 있는 모바일 네트워크와 연계하여 네트워크의 구축과 안정적인 키 인증 및 관리에 대한 보다 연구를 수행하고 있다.

참고문헌

[1] E. M. Royer and C. K . Toh, "A review of current Routing Protocols for Ad Hoc Mobile wireless Network", Proc. IEEE Personal Communication, 99, April 1999

[2] L. Zhou and Z. J. Haas, "Securing Ad Hoc networks", IEEE Network, Vol 13, No. 6, Nov, 1999

[3] Z. J. Haas, " A New Routing Protocol for the Re-configurable wireless network", http://www.ee.cornell.edu/ April 1, 2000

[4] Y. Desmedt, "Threshold Cryptography", European Transaction on Telecommunications", 5(4) : pp 449-459, July, 1994

[5] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar, "The Zone Routing Protocol(ZRP) for Ad Hoc Networks-IETF draft', 1997

[6] Charles Perkins, E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing"

[7] Ching_Chun Chiang, Hsiao-Kuang Wu, Wenston Liu, Mario Gerla, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel", 1997

[8] The Bluetooth Special Interest Group, Specification of Bluetooth System, vol. 1: Core, v1.0 B, Dec 1999

[저 자 소 개]

이 충 세 (Chung-Sei Rhee)

1973년 3월 학사
1979년 8월 University of South Carolina 석사
1989년 8월 University of South Carolina 박사

email : csrhee@cbnu.ac.kr