MANET 에서 Secure Property를 고려한 라우팅 프로토콜 연구

안영아[0], 최진영
고려대학교 컴퓨터학과
{ellaahn[0], choi}@formal.korea.ac.kr

Study of Secure Routing Protocol for Secure Property in MANET

Young-Ah Ahn[0], Jin-Young Choi,
Department of Computer Science & Engineering, Korea University

요약

MANET 환경에서 Secure Property를 만족하며 노드의 Connectivity 끊김 현상을 사전에 예견하고 또한 Power group을 형성하여 liveness을 지원한다. 또한 Authentication을 만족하기 위해 Localized Certificated 방식의 매카니즘을 이용하여 Secure 라우팅 프로토콜을 제안한다.

1. 서론

1.1 Ad Hoc 기반의 통신망

애드 혹 네트워크는 기반 구조가 없는 네트워크이다. 전통적인 네트워크와는 달리 기반 구조를 미리 배치하지 않고, 중앙 관리 라우터 혹은 종단간 라우팅을 지원하기 위한 엄격한 정책을 따르고 있다. 노드들은 자신의 라우팅 패킷에 의존하고 있으며, 노드들은 노드들간의 라우팅 패킷에 의존한다. 움직이는 노드는 다른 노드의 무선 범위와 직접적으로 통신할 수 있으나 노드들이 멀리 떨어져 있는 경우는 중간 노드의 라우트 메시지에 의존하여 통신한다[4]. 애드 혹 네트워크의 라우팅 프로토콜과 보안을 접목하여 애드 혹 통신망에서의 보안 취약점을 분석한 후 이를 해결할 수 있는 보안 프로토콜을 제안한다.

1.2 Secure Property

보안 속성은 다음과 같다[1]

*기밀성(Confidentiality)*은 전송된 정보는 정당한 수신자만 액세스 되는 것을 보장해야 한다. *인증(Authentication)*은 상대방의 ID 인증을 보장하고 통신을 허락한다. *무결성(Integrity)*은 전송하는 동안 변조되지 않는 것을 보장한다. *부인 방지(Non-repudiation)*는 상대방에 의해 정보의 전송과 정보를 받는 것을 검증하는 것을 보장한다. 즉 부분은 데이터 송신이나 수신을 부인할 수 없다. *가용성(Availability)*은 의도된(intended) 네트워크에서 의도된 네트워크 서비스는 요구 되어진 의도된 부분에서 가용한 서비스를 보장한다.

위의 property 중에서 Non-repudation은 라우팅에서는 의미가 없다. 또한 일반적으로 Confidentiality는 라우팅 프로토콜에서는 고려하지 않는다.[4] 하지만 여기에서는 Confidentiality, Integrity는 일반적인 security requirement이고 Authentication은 한 hop마다 인증 매카니즘을 지원하는 접근 방법이[2] 있다.
Confidentiality, Integrity의 경우 cryptographic mechanism을 이용하여 property을 만족한다.

본 논문에서는 Confidentiality와 Integrity를 만족하기 위해 key management를 쓰고 Authentication을 만족하기 위해 self-organized Key management의 Localized Certificated [9] 방법을 쓰고자 한다.

1.3 Secure Routing Property

라우팅이란 source 노드에서 중간(intermediate) 노드를 거쳐서 destination까지 가야 하는 패스를 찾아야 한다. 그런데 중간 노드가 compromise 되면 compromise 노드는 라우팅 패킷을 재전송(retransmission) 하거나 변조시킬 수가 있다. 리다이렉션 공격은 경로 발견 메시지에서 홉 카운트 필드의 변경에 의한, AODV 프로토콜에서 가능하다. 라우팅 결정이 다른 측정 기준에 의해 만들어지지 않는다. AODV 최단 경로를 결정하기 위해 홉 카운트 필드를 사용한다. AODV에 있어서 악의를 가진 노드는 0까지 RREP의 홉 카운트 필드를 재설정하고, 관심 있는 노드로 향하게 한다. 비슷하게 무한대로 RREP의 홉 카운트 필드를 설정하게 되면, 경로는 새롭게 생성하게 되고 악의적인 노드는 포함되지 않는다. 그러므로 원하는 목적지로의 path를 찾을 수 없다. 또한 원하는 목적지로 패킷을 보낼 수 없다. 그러므로 중간 노드를 trust할 수 있도록 authentication requirement를 만족해야 한다. 본 논문에서는 self-organized certificated [4] 방법을 이용하고자 한다.

또한 Availability는 중요한 issue이다. 왜냐면 무선 환경에서 원하는 목적지에 패킷을 항상 전송할 수 있어야 한다. 또한

라우팅 정보가 확보되었다면 언젠가는 반드시 전송되어야 한다. 그러므로 일단 정해진 라우팅에 참여하는 노드들은 절대로 power 부족 상태가 발생해서 라우팅 중에 power off 상태나 processing time을 라우팅 하는데 다 소모해서도 안 된다. 그러므로 라우팅 path를 찾는 시점의 power의 량을 인지해서 일정한 threshold 이하가 되면 라우팅에 참여하면 안 된다. 항상 liveness를 지원하려면 각 노드는 서로의 power 정보를 주기적으로 공유하여서 dynamic 하게 power group을 형성해야 한다. 결국 power group을 통해서만 라우팅 path를 찾아야 한다.

또다른 requirement 는 load balancing이다. Power group을 통해서 라우팅 path를 찾으면 임의의 노드로 집중화 될 수 있다. 이럴 때 load를 분산시켜 주어야 한다. 그렇게 하려면 single path 라우팅이 아닌 multi-path 라우팅을 이용하면 된다. 단 multi-path를 설정할 때 서로 다른 노드를 지나도록 해야 할 것이다.

2. Self Organized Public-Key Management

2.1 A Certificated Graph

모바일 애드 혹 네트워크에서 공개 키 암호화 구조는 security 서비스를 지원하기 위한 일반적인 구조이다. 액티브 공격자의 존재 하에서 사용자 U가 다른 사용자 V에게 공개 키로 인증하는 것은 중요한 문제이다.
시스템은 다음과 같다고 가정한다.
사용자는 자신의 키와 인증서를 생성하며, 집중화된 인증 권한 부여는 없으며, 인증서 디렉토리도 없으며, 노드의 부분 집합에서 명세 된 룰의 할당도 없으며, 먼저 인스톨된 절차나 키도 없다.

모델로는 사용자 I가 주어진 사용자 J에게 속하는 주어진 공개 키를 믿는다는 가정을 한다.

인증 그래프 G(V, E)
V 는 키의 집합이고 E는 에지의 집합이고, (i, j)에 직접적인 에지를 추가한다. 만약 I는 공개 키 인증으로 $\{j, K_j\}prK_i$ 사용자 J에서 표시되어 졌다.

$\{j, K_j\}prK_i$

2.2 Self Organized Public Key Management

초기화 과정에서 사용자는 자기의 로칼 인증서 저장소를 구성한다. 즉 인증서의 집합을 저장한다.
그 다음 단계로는 사용자는 다른 사용자의 공개 키를 검증을 얻기를 원한다. 사용자는 자신의 로칼 저장소를 합병하고 인증서 그래프들 사이에서 인증서의 패스를 찾기 위한 작업을 한다.

각 사용자는 공개 키 인증서를 로칼 저장소에 저장한다. 이는 서브 그래프이다. 이 작업은 바깥으로 나가는 edges는 이슈된 인증서를 저장하고, 들어오는 edges는 다른 이슈 된 인증서의 리스트를 저장한다. 임의의 알고리즘 A에 따라서 선택 되어진 인증서의 추가적인 집합을 저장한다.
사용자는 자신의 저장소를 생성하기 위해 동일한 알고리즘을 사용한다. 키를 검증하기 위해 로칼 저장소를 합병한다.
노드는 자신의 incoming과 outgoing 패스에서 높은 차원의 디그리를 가진 노드를 선택한다.

시스템의 성능을 정의하기 위해

$$P_A(s,G) = \frac{|\{(u,v) \in V \times V : K_u \rightarrow {}_{G_{add} \cup G_{rm}} K_v\}|}{|\{(u,v) \in V \times V : K_u \rightarrow {}_{G} K_v\}|}$$

설계의 목표는 계정에서의 인증 매트릭 사용의 재정의 되는 성능과 키 재사용시 모든 정점은 매번 같은 횟수의 인증을 위해 사용 되어지는 것을 필요로 한다. 또한 확장성은 로칼 저장소의 크기(서브그래프)와 통신 비용을 최소화한다. 또한 그래프 변화에도 인증은 변함이 없어야 한다.

3. Load-Balanced Power Group

3.1 LABR(Load-Balanced Wireless Ad Hoc Routing)

LABR 프로토콜[11]은 애드 혹 네트워크 환경에서 부하 균등을 고려한 대표적인 라우팅 프로토콜이다. LABR은 네트워크의 트래픽 상태를 고려하여 가장 트래픽 로드가 작은 경로를 찾아내는 것을 목적으로 한다.

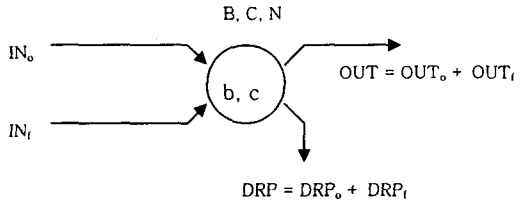
1) 네트워크에 브로드캐스트
2) 트래픽 로드에 대한 상태 정보를 수집
3) 수신된 메시지들 중에서 가장 비용이 작은 경로를 골라 확인 메시지를 소스에게 전송
4) 수신한 목적지 노드는 자신이 유지하고 있는 경로 정보 중에서 새로운 경로를 다시 선택하여 확인 메시지를 전송함으로써 우회 경로를 설정한다.

시간에 따라 네트워크 상태가 수시로 변화하는 애드 혹 네트워크 환경에서는 잘못된 경로 선택의 가능성이 높아진다고 할 수 있다. 또한 Power 상태를 고려하고 있지 않다.

3.2 Power Group

애드 혹 네트워크에서 라우팅은 임의의 노드가 라우팅을 집중적으로 처리해야 하는 경우가 발생한다. 이때 각 노드는 자신의 power 상태에 따라 더 이상의 라우팅 패킷 forwarding을 하지 않고 drop 시키면서 마치 다른 노드에게는 forwarding 하는 것처럼 하는 현상을 selfishness [1] 라고 한다. 이런 현상은 망의 connectivity를 유지해 주기 위한 방법이지만 misbehavior한 행동의 원인이 된다.
이것을 해결하기 위한 방법으로 라우팅 프로토콜의 liveness를 지원하기 위한 power 그룹을 형성하여 파워

그룹만 라우팅에 참여하게 하는 방법이다.
먼저 각 노드가 가지고 있는 정보를 주기적으로 브로드캐스팅하여 알리는 유선 망에서의 방법이 아니라 라우팅 정보를 찾기 위해 AODV 같으면 RREQ 메시지에서 source power 정보를 넣어서 request한다. 패킷은 중간 노드를 거치면서 급속하게 확산된다. 앞에서 언급한 self organized public key management에서 certificate graph를 이용하여 각 노드의 초기 배터리 레벨과 초기 신용 레벨, 상수 비용을 이용하여 인증 그래프와 함께 power 그룹을 형성한다.



"Nuglets"모델[1]로서 B는 초기 배터리 레벨이고 C는 초기 신용 레벨이며, N은 상수 비용이다. B는 배터리이고 c는 신용 카운터이다.
OUT_o 는 전체 라이프타임 동안 자신의 패킷을 송신하는 것이다. OUT_f는 전체 라이프 타임 동안 패킷을 송신을 포워딩 하는 것이다.
여기서 OUT_o가 최대가 되기 위한 조건으로

1) $OUT_o, OUT_f >= 0$
2) $N\,OUT_o - OUT_f <= 0$
3) $OUT_o + OUT_f = B$

이어야 한다.

4. 결론 및 향후 연구 방향

본 논문에서는 애드 혹 네트워크의 라우팅 프로토콜에 secure 한 속성(Confidentiality, Authentication, Integrity, Availability)을 만족하는 라우팅 프로토콜을 제안하였다. 특히 Authentication을 만족하기 위하여 self-organized key management 의 local certificated graph의 방법을 채용하였고 node의 끊김 방지인 connectivity와 liveness를 지원하기 위해서 power group을 Nuglets방식을 채용하였다. 애드 혹 네트워크에서는 노드의 trust를 인증하는 방식과 노드의 부하를 균등하게 가져가는 방법은 별도로 연구되어 지고 있다. 또한 본 논문에서는 부하 균등을 지원하면서 노드의 끊김 예견을 power group이라는 형태로 지원하였다. 향후 연구 과제로는 이 제안한 방법을 시뮬레이션을 통해 성능을 평가해 보며 포말 검증을 통해 security requirement를 만족하는 지를 연구하고자 한다.

5. 참고문헌

[1] Jean-Pierre Hubaux, Security of Wireless Ad Hoc Networks, 2002
[2] L.Zhou and Z.Haas, "Securing Ad Hoc Netowrks", IEEE Networks, Nov./Dec. 1999
[3] B.Dahill, B.Levine, E.Royer, and C.Shields, "A Secure Routing Protocol for Ad Hoc Networks", UMass Technical Report CS-2001-037, August, 2001
[4] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks", CNDS 2002
[5] S.Marti, T.J. Giuli, K.Lai, and M. Baker, "Mitigating Routing in Self-Organizing Mobile Ad Hoc Networks", Accepted for publication in ACM Journal for Mobile Networks(MONET), special issue on Mobile Ad Hoc Networks, 2003
[6] Y.Zhang and W. Lee, "Intrusion Detection for Wireless Ad-Hoc Networks", MobiCom 2000
[7] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks", MobiCom 2001
[8] Songwu Lu, "Network-centric Security Design for Mobile Ad Hoc Networks", MobiHoc 2002
[9] Srdan Capkun et al, "Self-Originized Public-Key Management for Mobile Ad Hoc Networks", MobiHoc 2002
[10] Zygmunt J. Haas et al, " Secure Routing and Transmission Protocol for Ad Hoc Networks", MobiHoc 2002
[11] Claude Castelluccia, "Crypto-Based ID in MANET: some preliminary thoughts", Working Session on Security in Ad Hoc Netwoks, EPFL, Lausanne, June 12, 2002