보안 애드 혹 네트워크를 위한 동적인 토큰 분배 프로토콜

이재식*, 김성천*
*서강대학교 컴퓨터공학과
e-mail : ljsljslove@sogang.ac.kr, ksc@sogang.ac.kr

Dynamic Token Escrow Set Protocol for Secure Ad Hoc Networks

Jae Sik Lee*, Sung Chun Kim*
*Dept of Computer Science & Engineering, Sogang University

요 약

애드 혹 네트워크는 Wireless network의 특성 상 보안에 취약하고 또한 기존의 보안 솔루션을 적용하기 어렵다는 문제점을 가지고 있다. 이러한 애드 혹 네트워크에서의 보안 상 문제점을 해결하기 위한 Token Escrow방식을 살펴보고, 확장성 있는 Token 분배 방법을 통하여 발전된 기법을 제안한다.

1. 서론

최근 여러 분야에서 무선기기의 발명과 보급으로 다양한 모바일 애드 혹 네트워크가 구성되고 있다. 이러한 환경에서 사람들은 무선 네트워크를 통하여 중요한 정보나 데이터를 전송하고 받게 된다. 때문에 이러한 정보는 기밀성과 보안성이 유지되어야 한다. 하지만 애드 혹 네트워크의 특성상 공기 중으로 전파를 쏘는 방식이기 때문에 보안에 취약할뿐더러, 기존의 유선 환경에서 사용되던 다양한 보안 솔루션을 직접 적용시키는데도 문제가 있다. 이에 따라 최근 애드 혹 네트워크에서의 보안 솔루션이 크게 부각되고 있다.

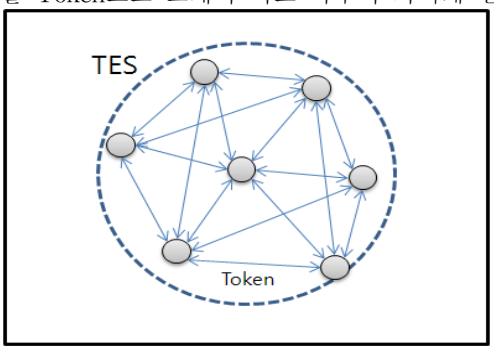
2. 기존 연구

2.1 SAODV

SAODV 기법은 Hash Chain을 이용하여 경로상의 문제가 있는지를 검증할 수 있도록 하는 방법이다. Source 노드에서 RREQ를 플러딩할 때, 노드는 자신의 고유 인증 값을 Hash function을 통해 변환한 뒤 다음 노드에게 전송한다. 중간 노드는 이를 받아 자신의 테이블에 저장한 후 RREQ에 자신의 인증 값을 Hash function을 통해 변환한 값을 붙여 다음 노드에게로 플러딩한다. 이와 같은 과정을 거치면서 Destination 노드에 도착한 경로 요청 메시지는 지나온 경로에 속하는 노드들의 Hash 변환 인증 값의 Chain을 가지게 된다. Destination 노드는 RREQ를 전송받은 후 해당 메시지의 인증 값을 검사한다. 만약 RREQ 패킷이 타당하면 RREP 패킷을 전송한다. 중간 노드가 RREP를 수신하면 인증키를 확인하고 이상이 없는 것을 확인한 노드는 해당 노드를 자신의 다음 Path로써 인증하게 된다. Source 노드에까지 RREP가 도착하면 Source 노드는 Data packet을 전송하게 되는데 이 때 Hash되지 않은 인증 값을 함께 전송하고, 중간 노드들 역시 Data packet에 붙여서 전송하게 된다. Destination에서 Data packet을 받으면 인증 값의 Chain을 가지게 되는데 이를 Hash 하여 RREQ에 포함되었던 Hash Chain과 비교, Data packet의 무결성을 입증하게 된다.

2.2 SRPTES

SRPTES는 SAODV에서 사용되는 인증 값을 보호하기 위한 기법이다. 노드가 고유의 인증 값을 Attacker에게 빼앗기는 경우 Malicious 노드가 마치 정당한 노드인 양 네트워크에 침입하여 통신을 방해할 수 있다. 따라서 이러한 인증 값을 Token 단위로 쪼개어 자신의 주변 노드들과 나누어 가지는 것이다. 이를 위해 Token을 나누어 갖는 그룹 TES를 만들고, TES member들 끼리 서로 자신의 인증 값을 Token으로 쪼개어 서로 나누어 가지게 된다.



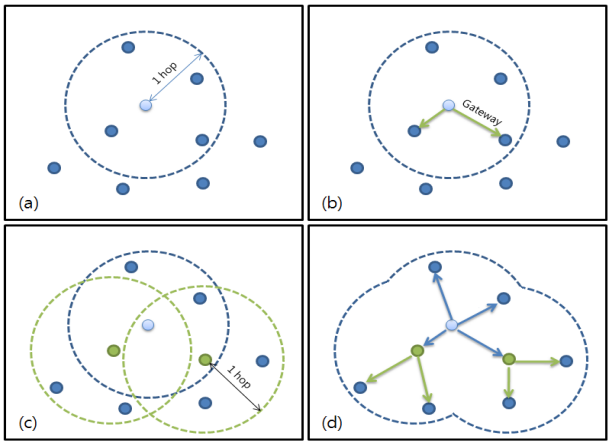
(그림 1) SRPTES의 Token Escrow

이 때 (n, k) Secret Sharing 기법을 사용하게 되므로 TES의 노드의 수는 처음 구성 노드를 포함한 n개로 제한이 된다. 또한 인증 값과 더불어 Group key를 전송하여 Token 전송에 이상이 없는지를 검사하게 된다. 라우팅을 위하여 인증 값의 Token을 모두 모은 Source 노드는 SAODV의 방식과 마찬가지로 Hash Function을 이용하여 인증 값을 Hash하고 Hash Chain을 이용하여 데이터의 보

안을 보장하게 된다.

3. 제안 기법

기존의 SRPTES는 TES의 크기를 n개로 고정시킴으로써 Secret Sharing 기법을 사용하고 있다. 하지만 TES 구성 노드 주변의 노드 개수가 n개 이하인 경우 TES를 구성하지 않게 되어 해당 노드들의 인증 값 보호에 문제가 생기게 된다. 이를 해결하기 위해 TES 구성 노드 이외에 TES Gateway 노드를 선정하는 기법을 제안한다. n개 이하의 노드를 가지는 지역에서는 TES의 크기를 Static하게 구성 노드의 1 hop으로 제한하지 않고 확장시키는 것이다. 이를 위해 TES 구성 노드는 자신을 포함한 주변의 노드 개수가 n개 미만인 경우 주변 노드들에게 Gateway가 될지 여부를 묻는 메시지를 전송한다. 이를 받은 노드들은 자신의 주변 노드들을 살펴보고 TES member로 귀속 시킬 노드가 발견되는 경우 TES 구성 노드에게 Gateway를 하겠다는 메시지를 보낸다. 동시에 자신의 범위에 있는 무소속 노드들에게 자신의 TES로 들어올 것을 요청하는 메시지를 보내어 TES member로 귀속시키게 된다. 이에 따라 TES의 크기를 넓게 조정하여 n개 만큼의 TES member를 가지도록 한다.



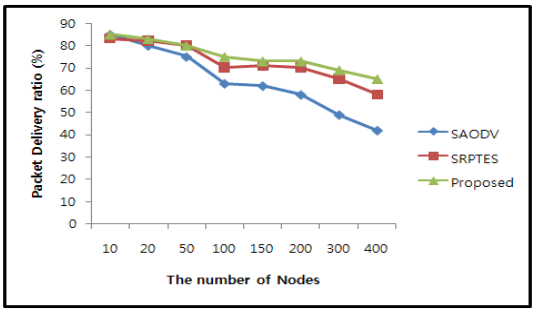
(그림 2) TES 확장의 단계별 순서

이 때 TES의 Token 전달은 모두 Gateway 노드를 통하여 전송되게 되어 Tree 구조의 Token 전달 구조를 가지게 된다.

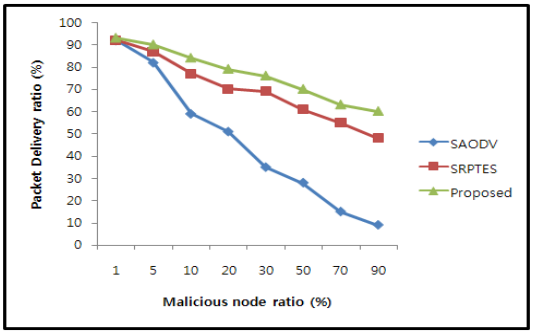
위와 같은 일련의 과정을 통하여 네트워크의 모든 노드들이 자신의 인증 값을 주변 TES에 나누어 맡겨둠으로써 Attacker의 공격으로부터 보다 안전하게 지킬 수 있게 된다.

4. 시뮬레이션

해당 기법의 시뮬레이션은 다음과 같은 실험을 통해 수행된다. Malicious 노드가 존재하는 네트워크에서 노드의 개수가 10, 20, 50, 100, 150, 200, 300, 400으로 증가할 때 패킷의 전송 성공률, Malicious 노드의 비율에 따른 패킷의 전송 성공률 등의 실험을 통하여 제안 기법이 SAODV 혹은 SRPTES에 비해 보다 안정적이고 신뢰성 있는 전송이 가능함을 볼 수 있었다.



(그림 3.a) 노드의 수에 따른 전송 성공률



(그림 3.b) Malicious 노드 비율에 따른 전송 성공률

5. 결론

애드 혹 네트워크는 앞으로도 다방면의 연구가 이루어질 것이라고 판단된다. 하지만 그만큼 정보와 데이터를 파괴, 혹은 감청, 악용하기 위한 Attacker들의 방법 역시 다양화될 것이다. 100% 완벽한 보안 기법은 존재하지 않는다. 하지만 제안된 기법을 통하여 애드 혹 네트워크의 보안에 대해 100%의 보안을 목표로 발전시켜 나간다는 것이 중요하다고 생각한다. 앞으로도 다양한 연구와 보완을 통하여 더욱 완벽한 보안 기법을 이룰 수 있도록 연구해나가야 할 것이다.

ACKNOWLEDGMENTS

이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2009-0075881)

참고문헌

[1] Chen Huang, Benxiong Huang, Yijun Mo and Jianhua Ma *"SRPTES: A Secure Routing Protocol Based on Token Escrow Set for Ad hoc Networks,"* AINA 2008, 22nd International Conference on.

[2] Yih-Chun Hu and Adrian Perrig *"A Survey of Secure Wireless Ad Hoc Routing,"* IEEE Security & Privacy, pp.28-39, May/June 2004.

[3] S.Gupte and M.Singhal *"Secure Routing in Mobile Wireless Ad Hoc Networks,"* Elsevier, Ad Hoc Networks, pp.151-174, 2003.