제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

무선 애드 혹 네트워크에서 에너지 효율적인 Token Escrow 트리 기반의 보안 라우팅 프로토콜

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

An Efficient Secure Routing Protocol Based on Token Escrow Tree for Wireless Ad Hoc Networks

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

요 약

최근 무선 네트워크 기술이 점차 각광을 받으면서 다양한 애드 혹 환경에서의 라우팅 프로토콜이 제안되고 있다. 하지만 애드 혹 네트워크라는 환경의 특성 상 보안상 취약한 문제점을 가지고 있으며, 기존의 유선 네트워크 환경에서 제안되었던 보안 라우팅 프로토콜을 적용시키기 힘들다는 문제점이 있다. 이에 따라 보안성을 보완한 새로운 애드 혹 라우팅 프로토콜이 제안되었지만 다양한 무선 네트워크 환경의 변화에 유동적으로 대응하기 힘들고 보안적인 측면에 집중을 한 나머지 에너지소모 측면에서는 단점을 노출하고 있다. 본 논문에서는 다양한 애드 혹 네트워크 환경에 적용 가능하고, 기존의 보안 라우팅 프로토콜에 비해 에너지 효율적인 보안 라우팅 프로토콜을 제안하고자 한다. 보안 정보의 보호를 위해 Tree 구조를 도입하고 보안 단계를 통한 Multi-path를 구성하여 악의적인 노드의 Dropping Attack에 대비하고, 예기치 못한 Data Packet의 손실에 대해서도 효율적으로 대처하게 하였다. 실험 결과 악의적인 노드가 존재하는 네트워크 환경에서 기존의 애드 혹 네트워크 보안 라우팅 프로토콜보다 21%정도의 패킷 전송 성공률을 높일 수 있었으며 또한 각 노드의 에너지를 균등하게 소모함으로써 전체적인 네트워크의 생존시간이 연장되는 것을 확인할 수 있었다.

1. 서론

무선 애드 혹 네트워크 기술은 중앙 시스템의 도움 없이 각각의 통신 기기 간에 데이터를 주고받는 네트워크이다. 과거에는 주로 군사적인 목적을 위해 중앙 시스템을 구축하기 힘든 전투 지역에서 개별적인 무선 단말들 간 서로 정보를 전달하고 통신을 유지할 수 있도록 사용되거나, 산간지역이나 재해지역과 같이 유선 환경이 구축이 어려운 환경에서 통신을 위해 사용되었으나, 최근에는 블루투스와 같은 모바일 기기에서의 활용 기술이 늘어남에 따라 일상생활에서 흔히 접할 수 있는 무선 네트워크 기술로 떠오르고 있다.

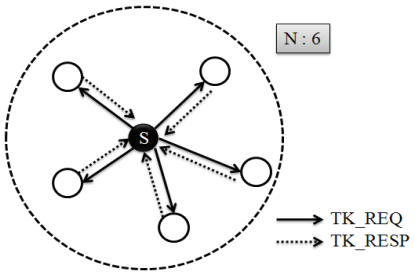
하지만 무선 애드 혹 네트워크는 노드의 신분이 서로에게 불확실한 경우가 많으며, 도청, 간섭, 혼선 등의 공격에 대해 공격받기 쉽다는 단점을 가진다. 또한 기존의 애드 혹 네트워크 프로토콜들은 모든 노드가 신뢰할 수 있다는 가정 하에 제안이 되었기 때문에 데이터 변조나 노드의 위장 공격, DoS 공격 등에 취약한 면을 보인다. 또한 노드 관리를 중앙에서 제어하지 않기 때문에 기존의 유선 네트워크 환경에서 적용되던 보안 기법을 적용시키는데 어려움이 있다. 더욱이 모바일 통신 기기는 프로세싱 에너지 측면에서 제약을 가지고 있다. 이러한 한계는 완벽한 보안 기법을 실질적으로 무선 애드 혹 환경에 적용시키기 힘들게 하는 원인이 된다.[1]

2. Token Escrow 기법

기존 애드 혹 네트워크의 보안 기법은 자기 자신의 Key 값이나 Seed 값, 서명 값 등에 대한 정보를 자신이 모두 저장하고 있다가 인증이 필요한 경우 사용을 하였다.[2],[3],[4] 때문에 직접 공격을 받아 보안정보를 강탈당할 경우에는 마땅한 해결책이 없었다. Token Escrow 기법은 이러한 문제를 해결하기 위해 자신의 보안 정보를 직접 저장하지 않고 다수의 제 3자가 보관하도록 하여 해당 노드가 공격당하는 경우에도 보안성을 유지하는 것을 목표로 하고 있다. 이러한 기법의 대표적인 예가 Secure Routing Protocol based on Token Escrow Set(SRPTES) 기법이다.[5]

SRPTES 기법의 동작방식을 보면, 우선 네트워크 구성 초기단계에서 각각의 노드들은 자신의 이웃노드들과

Token Escrow Set (TES)라고 정의된 자신의 보안 정보를 믿고 맡겨둘 집단을 구성한다.



(그림 1) TES를 구성하기 위한 Message Handshake

TES 구성이 완료된 후 각각의 노드는 해쉬 함수를 통해 변환시킬 자신의 Seed값을 생성하고 Threshold Secret Sharing 기법을 사용하여 해당 Seed를 Token 단위로 나눈다. 이렇게 나누어진 각 노드의 Token들은 자신을 포함한 자신의 TES 멤버 모두에게 하나씩 전송이 되고 이를 받은 노드는 전송받은 Token과 해당 노드의 ID를 저장한다.

이후, 경로 설정 단계에서 데이터 전송을 하기 위해 노드는 주변 TES 멤버들에게 자신의 Token을 돌려줄 것을 요청하는 메시지를 보내게 된다. Token 요청 메시지를 수신한 각 멤버 노드들은 Token을 원래의 노드에게 돌려주게 된다. 모든 Token 조각을 받은 노드는 Token을 재조립한 후, Threshold Secret Sharing 기법을 사용하여 Token과 초기의 Seed값을 비교확인하고, 올바른 값이 확인된 경우에 Routing Path를 구성하여 보안성이 보장된 통신을 이루어준다.

3. 제안 기법

3.1 Token Escrow 2-Level Tree

본 논문에서 제안하는 알고리즘의 기본 아이디어는 다음과 같다. TES를 구성할 경우 자신을 제외한 노드들에게 Token을 단순히 분배하여 나누어주지 않고, TES을 구성시 각각의 노드는 자신을 중심으로 Tree를 구성하여 Tree의 Leaf 노드들에게 자신의 Token을 분배하는 것이다. 이를 통해 공격자가 Token Escrow Tree의 구조를 파악하지 못하는 한 해당 그룹의 보안성을 보장해주는 것이 중요 목적이다. 또한 TES의 구성멤버 수(N)를 고정시키자 않고 구역에 따라 유동적으로 Tree 구조에 노드를 귀속시키기 때문에 노드의 분포도에 따라 TES에 속하지 못하는 노드가 생기거나, TES 구성이 되지 않는 경우를 방지한다.

Token Escrow 2-Level Tree를 구성하는 단계를 좀 더 구체적으로 설명하면 다음과 같다.

Step 1. 각 노드는 TES을 구성하기 위해서 [그림 2]과 같이 6개의 방향성을 가지고 각각의 구역에 Tree 구성 메시지(Tree_REQ)를 Broadcast한다.

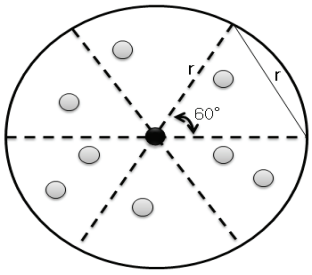
Step 2. Tree_REQ를 받은 노드는 자신의 ID를 포함한 Tree 응답 메시지(Tree_REP)를 Tree 구성 노드에게 전송한다.

Step 3. 이를 통해 Tree 구성 노드는 자신의 주변의 노드에 대해 ID 정보와 방향성을 알게 되고 이 정보를 6개의 방향에 따라 각각의 Queue를 생성하고 Tree_REP가 도착하는 순서대로 노드 ID를 Queue에 저장한다.

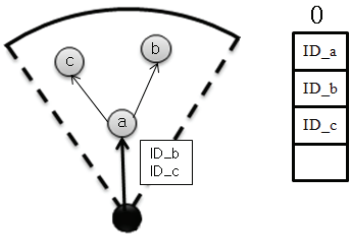
Step 4. Tree 구성 노드는 각각의 Queue Table에서 가장 먼저 도착한 노드의 정보를 읽고 해당 노드를 자신의 Child 노드로 선정한다. 이와 동시에 구성 노드는 해당 방향의 Queue Table에 저장되어 있는 나머지 정보를 Child 노드에게 전송한다.

Step 5. [그림 3]과 같이 Tree 구성 노드의 Child 노드(a)는 전송받은 정보를 바탕으로 나머지 노드들에게 자신이 Parent 노드임을 알리는 메시지를 전송한다.

Step 6. 메시지를 받은 노드들은 자신이 Leaf 노드인 것을 알게 되고 Parent 노드에게 귀속됨을 알리는 메시지를 전송 모든 노드가 종속됨을 확인한 Parent 노드는 Root 노드에게 Tree가 완성됨을 알리는 메시지를 보낸다.



(그림 2) Tree 구성을 위한 지역 분할



(그림 3) Queue Table을 이용한 Tree 구성

다음과 같이 Tree를 구성한 후 경로 설정 단계에서는 기존의 SRPTES 기법과 동일한 단방향 해쉬 알고리즘을 사용한다. 데이터 통신을 하고자 하는 노드가 Tree 구조를 통하여 자신의 Token을 모두 받아 원래의 Seed 값을 생성한 후 해당 노드는 RREQ를 전송하게 된다. 이 때 Seed 값을 해쉬 함수를 통해 변환한 값인 TAC을 RREQ에 함께 전송하게 된다. RREQ를 받은 중간 노드들은 소스 노드와 마찬가지로 Tree를 따라 자신의 Token을 모으고 합쳐진 자신의 Seed 값을 해쉬하여 RREQ에 추가하여 전송하게 된다. 이러한 수행을 거쳐 목적지 노드에 도착한

RREQ는 해당 경로에 속한 노드들의 TAC가 차례대로 저장된 TAC 체인 값을 포함하게 된다. RREQ가 전송된 후 목적지 노드는 해당 경로에 따라 RREP를 소스 노드로 전송하게 된다. RREP를 받은 소스 노드는 데이터 패킷을 전송하면서 해당 패킷에 자신의 Seed값의 원본을 붙여서 전달하게 된다. 중간 노드들 역시 소스노드와 마찬가지로 자신의 Seed값을 아무런 변환 없이 데이터 패킷에 추가하여 전송한다. 이렇게 목적지 노드까지 도착한 데이터 패킷은 Seed 값의 체인을 전달받게 되고, RREQ를 통해 저장된 TAC 체인과 데이터 패킷을 통해 전달된 Seed 체인의 두 가지 정보를 저장한다.

이후 목적지 노드는 전달된 Seed 체인을 해쉬 함수를 통해 변환시키고 해당 체인의 내용이 RREQ를 통해 전달된 TAC 체인의 값과 같은지 여부를 살펴본다. 만약 Seed 체인의 변환 값과 TAC 체인의 값이 동일하다면 해당 경로를 통한 데이터 패킷은 아무런 위조나 변조 없이 정상적으로 전달되었다고 판단한다.

3.2 Multipath Routing Protocol

다중 경로를 설정하기 위해 RREQ가 전송될 때 소스 노드는 목적지 노드, Seed 값을 변환한 TAC 값 등의 기본 정보에 추가로 자신의 보안 레벨을 함께 전송한다. 목적지 노드에서는 첫 번째 RREQ가 도착한 후 바로 해당 경로를 통해 RREP를 전송하지 않고 일정 시간동안 다른 경로를 통해 도착하는 추가적인 RREQ가 도착하는 것을 기다린다. 여러 경로를 통한 RREQ가 도착한 후 목적지 노드는 크게 다음과 같은 세 가지의 기존에 의해 분류된 경로를 통해 RREP를 전송하게 된다.

① 홉 수만을 고려한 최단 경로
② 홉 수와 함께 보안 레벨을 함께 고려한 경로
③ 보안 레벨이 가장 높은 보안을 최우선한 경로

이러한 각각의 경로를 선별하기 위해 본 논문에서는 다음의 수식을 통해 해당 경로를 계산하고자 한다. 먼저 보안 레벨과 홉 수를 동시에 고려한 ② 경로를 찾아내기 위하여 수식 (1)과 같은 계산을 통해 경로를 선택한다.

$$P = \mathrm{argmax}_{i \in R}[(1-\alpha) \times \frac{E(SL_i)}{\delta(SL_i)} + \alpha \times \frac{1}{Hopcount}] \quad (1)$$

수식 (1)에서 R은 RREQ가 전달된 경로의 노드 집합을 나타내고 E(SLi)는 해당 경로의 각 노드에 대한 보안 레벨의 평균, δ(SLi)는 경로의 노드에 대한 보안 레벨의 표준 편차이다. 보안 레벨의 평균뿐만 아니라 표준 편차까지 고려한 이유는 경로를 이루는 노드들 중 다른 노드들이 보안 레벨이 월등히 높고 현저하게 레벨이 낮은 노드가 존재하는 경우 즉, 전체적인 경로의 보안 레벨 평균은 높지만 악의적인 노드가 있는 경우를 고려하기 위함이다. 또한 Hcount는 경로를 지나온 홉 수, 그리고 α는 홉 수와 보안 레벨의 가중치를 결정하기 위한 변수로써 $0 < \alpha < 1$의 범위를 가진다. α의 값이 1인 경우는 홉 수가 가장 적은 최단 경로 ①이 되고, α의 값이 0인 경우 다음 수식 (2)와 같이 구성되며 이러한 식은 보안 레벨이 가장 높은 경로인 ③번 경로를 결정하는 수식이 된다.

$$P = \mathrm{argmax}_{i \in R}[\frac{E(SL_i)}{\delta(SL_i)}] \quad (2)$$

수식 (2)에서 R은 수식 (1)과 마찬가지로 RREQ가 전달된 경로의 노드 집합, E(SLi)는 해당 경로의 각 노드에 대한 보안 레벨의 평균, δ(SLi)는 경로의 노드에 대한 보안 레벨의 표준 편차가 된다.

세 개의 경로를 통해 소스 노드에 도착한 RREP는 소스 노드에 의해 서로 비교대상이 된다. 각각의 RREP에 담긴 목적지 노드에 대한 정보가 동일한 경우 일단 RREP가 전송되는 동안 공격자에 의해 목적지 정보가 변조되지 않았다는 판단 하에 가장 짧은 최단 경로인 첫 번째 경로를 통하여 데이터 패킷을 전송한다. 만약 최단 경로를 통해 도착한 RREP와 보안 레벨을 고려한 나머지 두 경로의 RREP가 불일치하는 경우에는 홉 수와 보안 레벨을 모두 고려한 경로를 통해 데이터 패킷을 전송한다. 또한 세 경로를 통해 도착한 RREP의 목적지 노드에 대한 정보가 서로 다 다른 경우 소스 노드는 수식 (2)을 통해 계산된 보안 레벨이 가장 높은 노드를 연결한 경로로 데이터 패킷을 전송한다.

4. 시뮬레이션

제안기법의 실험은 <표 1>, <표 2>에서 제시된 환경에서 Glomosim 2.03을 이용하여 수행하였다.

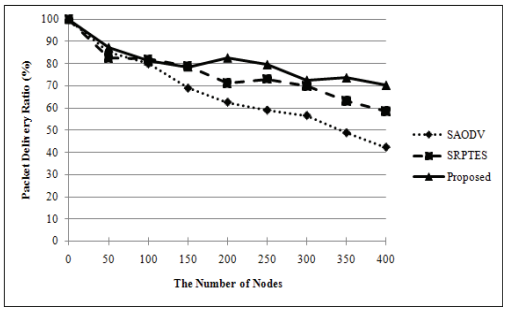
<표 1> 무선 애드 혹 네트워크 노드 환경

MAC Protocol	Mac / 802.11
Traffic Pattern	CBR
Size of data packet	70 Bytes
Interface queue type	Drop-Tail, Priority Queue
Initial Energy	10 J

<표 2> 시뮬레이션 필드 환경

Simulation Area	1500m X 1500m
Number of Nodes	50, 100, 150, … , 400
Simulation Time	100 seconds

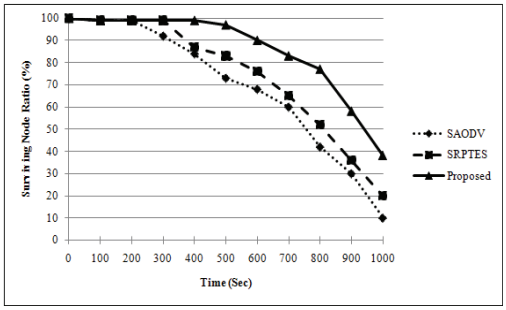
다음 실험 결과는 보안 라우팅 프로토콜에 대한 실험이기 때문에 악의적인 노드가 존재하는 환경에서, 얼마만큼 악의적인 노드에 영향을 받지 않고 정상적으로 소스 노드로부터 목적지 노드까지 데이터 패킷을 정상적으로 전달하는지를 살펴보면 보안상 안전한 기법인지에 대한 여부를 판단할 수 있다.



(그림 4) 노드의 수에 따른 패킷 전송 성공률

(그림 4)에서 x 축은 전체 네트워크에 분포된 노드의 수이고, y 축은 패킷 전송 성공률이다. 제안하는 알고리즘은 거의 모든 개수의 네트워크 환경에서 SAODV보다는 안정적인 결과를 나타냄을 볼 수 있으며 200개의 노드를 가지는 네트워크 이상의 환경에서는 SRPTES 기법보다 평균적으로 10%정도 높은 전송 성공률을 보여줌을 볼 수 있다. 이는 노드의 개수가 많아질수록 SRPTES에서 TES에 포함되지 못하는 노드가 생기는 반면 제안 기법에서는 최대한의 노드가 Tree 구성 멤버로써 자신의 보안 정보를 지킬 수 있는 환경이 구축되기 때문이라고 분석할 수 있다.

전체 네트워크의 생존 시간은 각 노드의 에너지 비율이 10% 이하로 내려갔을 때 정상적으로 동작할 수 없다고 가정, 10% 이하의 노드에 대해서는 네트워크에서 배제시키고, 이렇게 네트워크에서 배제된 노드 이외에 노드들은 생존 노드로 인식한다.



(그림 5) 전체 네트워크의 평균 생존 시간

(그림 5)을 보면 SAODV와 SRPTES의 경우에는 시간이 얼마 지나지 않아 10% 미만의 에너지를 가진 노드가 나타나게 되어 네트워크에서 배제되는 것을 살펴볼 수 있다. 시간이 지날수록 두 기법의 노드들은 에너지를 급격하게 잃어가는 것을 볼 수 있으며 800초 이후에는 전체 노드 중 생존 노드의 비율이 40%, 50%정도 밖에 남아 있지 않게 되어 네트워크로서의 기능을 제대로 수행할 수 없는 것 볼 수 있다.

5. 결 론

기존 애드 혹 네트워크의 보안 라우팅 알고리즘에서는 보안 정보를 통해 주변 노드와 인증을 하는 방식이나 혹은 이러한 보안 정보를 주변 노드에게 분산시켜 공격자의 직접 공격에 대비하도록 하는 등의 기법이 연구되었다. 하지만 네트워크의 초기화 단계부터 정상적인 노드인 것처럼 위장하고 있다가 데이터 패킷이 전송되는 시점에 악의적인 노드로 돌변하여 패킷을 빼앗아 가거나 삭제해 버리는 등의 공격이 이루어지는 경우 정상적인 애드 혹 네트워크 환경이 구축될 수 없는 상황이 발생한다. 본 논문에서 제안하는 알고리즘은 이와 같은 문제를 해결하고자 Token Escrow Tree를 구성하여 분배함으로써 Seed 값의 보호 효과를 최대화 할 수 있었다. 또한 보안 단계에 따라 세 경로를 구성하여 소스 노드가 초기에 선택한 경로를 통해 전송하였을 때 문제가 생기는 경우 선택 경로보다 보안성이 뛰어난 차선의 경로로 전송하게끔 함으로써 악의적인 노드로 인해 데이터 패킷이 정상적으로 전송되지 못하게 되는 경우를 최소화 하였다.

ACKNOWLEDGMENTS

본 연구는 한국과학재단 2009년 일반연구자지원사업 (No. 2009-0075881) 지원으로 수행되었음.

참고문헌

[1] G. Peng and Z. Chunanyun, “Routing Attacks and Solutions in Mobile Ad hoc Networks,” Proceeding of IEEE Communication Technology, ICCT'06, pp. 1 - 4, Nov. 2006

[2] Y. Seung, N. Prasad, and K. Robin, "Security-aware ad hoc routing for wireless networks," Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc 2001, pp. 229 - 302, 2001

[3] H. Yih-Chun, P. Adrian, and David B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Proceeding of Wireless Networks, Vol. 11, No. 1 - 2, pp. 21 - 38, Jan. 2005

[4] M. Guerrero, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," Journal of Imtermet Draft, IETF, Vol 06, pp. 106 - 107, Jul. 2002

[5] C. Huang, B. Huang, Y. Mo, and J. Ma, "SRPTES: A Secure Routing Protocol Based on Token Escrow Set for Ad Hoc Networks," Proceeding of IEEE Advanced Information Networking and Applications (AINA) 2008, pp. 583 - 589, Mar. 2008

[6] N. Unshona and W. T. Penzhorn, "Towards the Security of Routing in Ad Hoc Networks," Journal of IEEE ISIE 2005, Vol 4. pp. 1783 - 1788, Jun. 2005

[7] Yih-Chun Hu, Adrian Perring, and David B. Johnson, "Wormhole Attacks in Wireless Networks," Journal of IEEE on Selected Areas in Communications, Vol. 24, No. 2, pp. 370 - 380, Feb. 2006