pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.4.155

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

Lee Jae Sik† · Kim Sung Chun††

ABSTRACT

Routing protocol in ad hoc mobile networking has been an active research area in recent years. However, the environments of ad hoc network tend to have vulnerable points from attacks, because ad hoc mobile network is a kind of wireless network without centralized authentication or fixed network infrastructure such as base stations. Also, existing routing protocols that are effective in a wired network become inapplicable in ad hoc mobile networks. To address these issues, several secure routing protocols have been proposed: SAODV and SRPTES. Even though our protocols are intensified security of networks than existing protocols, they can not deal fluidly with frequent changing of wireless environment. Moreover, demerits in energy efficiency are detected because they concentrated only safety routing. In this paper, we propose an energy efficient secure routing protocol for various ad hoc mobile environment. First of all, we provide that the nodes distribute security information to reliable nodes for secure routing. The nodes constitute tree-structured with around nodes for token escrow, this action will protect invasion of malicious node through hiding security information. Next, we propose multi-path routing based security level for protection from dropping attack of malicious node, then networks will prevent data from unexpected packet loss. As a result, this algorithm enhances packet delivery ratio in network environment which has some malicious nodes, and a life time of entire network is extended through consuming energy evenly.

Keywords : Ad Hoc Networks, Secure Routing Protocol, Token Escrow Tree

무선 애드 혹 네트워크에서 보안성을 고려한 Token Escrow 트리 기반의 효율적인 라우팅 프로토콜

이 재 식† · 김 성 천††

요 약

최근 무선 네트워크 기술이 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 Secure AODV나 SRPTES 등의 보안성을 고려한 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 대비하여, 예기치 못한 Data Packet의 손실에 대해서도 효율적으로 대처하게 하였다. 실험 결과 악의적인 노드가 존재하는 네트워크 환경에서 기존의 애드 혹 네트워크 보안 라우팅 프로토콜보다 패킷 전송 성공률을 21%정도 향상시킬 수 있었으며 또한 각 노드의 에너지를 균등하게 소모함으로써 전체적인 네트워크의 생존시간이 연장되는 것을 확인할 수 있었다.

키워드 : 애드 혹 네트워크, 보안 라우팅 프로토콜, Token Escrow 트리

1. 서 론

무선 애드 혹 네트워크 기술은 중앙 시스템의 도움 없이 각각의 통신 단말 간에 데이터를 주고받는 네트워크이다. 최근에는 블루투스와 Wi-Fi와 같은 다양한 활용 분야가 늘어남에 따라 무선 네트워크 기술이 없는 일상생활을 상상할 수 없을 만큼 실생활에서 매우 중요한 부분을 차지하고 있다.

※ 이 논문은 2007년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2007-313-D00533).
† 준 회 원 : 서강대학교 컴퓨터공학과 공학석사
†† 정 회 원 : 서강대학교 컴퓨터학과 교수
논문접수 : 2013년 1월 29일
수 정 일 : 1차 2013년 3월 11일
심사완료 : 2013년 3월 11일
* Corresponding Author : Kim Sung Chun(ksc@sogang.ac.kr)

하지만 무선 애드 혹 네트워크는 노드의 신분이 서로에게 불확실한 경우가 많으며, 도청, 간섭, 혼선 등의 공격에 대해 공격받기 쉽다는 단점을 가진다. 특히 기존의 애드 혹 네트워크 프로토콜들은 모든 노드가 신뢰할 수 있다는 가정 하에 제안이 되었기 때문에 데이터 변조나 노드의 위장 공격, DoS 공격 등에 취약한 면이 있으며 모바일 노드는 프로세싱 에너지 측면에서 제약을 가지고 있다. 또한, 노드 관리를 중앙에서 제어하지 않기 때문에 기존의 유선 네트워크 환경에서 적용되던 보안 기법을 그대로 적용시키기에는 무리가 있다. 그렇기 때문에 안정성 있는무선 네트워크 프로토콜을 위한 추가적인 연구가 반드시 필요하다[1]

애드 혹 네트워크에서 기존 라우팅 기법들의 보안적인 문제를 해결하기 위하여 제안된 기법들로는 SAR, Ariadne, Secure AODV 등이 있다. 이러한 기법들은 보안 정보를 직접 자신이 저장하여 다른 노드와의 통신을 통해 자신의 무결성을 입증하는 방식이다. 또한 위의 기법들에서 발생할 수 있는 악의적인 노드에 의한 보안 정보의 강탈을 방지하기 위하여 기존에 자기 자신이 가지고 있는 노드의 보안 정보를 주위의 다른 노드들에게 분산시켜 관리하는 Escrow방식도 제안되었다.

본 논문에서는 기존의 Escrow 기법의 보안성 향상을 위하여 Tree 구조를 통해 보다 체계적으로 각 노드의 보안 정보를 주위의 다른 노드에게 분배하여 악의적인 노드에 의한 보안정보 강탈을 방지하는 보호기법을 제시한다. 또한 노드들의 보안 정보를 기반으로 경로의 보안 레벨을 설정하여 경로 구성 단계에서 보안 레벨에 따른 세 개의 경로를 구성하는 Multi-Path 라우팅을 통해 악의적인 공격에 보다 안정적으로 대응할 수 있는 기법을 제안한다.

2. 기존의 보안 라우팅 프로토콜

2.1 무선 애드 혹 네트워크에서 보안 정보를 이용한 라우팅 기법

애드 혹 네트워크에서 기존 라우팅 기법들의 보안적인 문제를 해결하기 위하여 RREQ, RREP, 데이터 패킷으로 구분되는 패킷 전송 단계의 보안성을 위해 SAR, Ariadne, Secure AODV 기법 등이 제안되었다.

SAR 프로토콜[2]은 AODV 기반의 보안 라우팅 프로토콜로, 각자의 애드 혹 노드의 보안 정보를 이용해 안전한 보안 경로를 설정한다. SAR은 기존의 라우팅 기법을 애드 혹 노드의 신뢰 레벨에 따라 노드간의 신뢰 관계를 형성하고, 정확한 보안 값을 수치로 표현하는 것이 특징이다. 만약 소스 노드와 목적지 노드 사이의 경로에서 신뢰 레벨이 낮은 노드를 발견하는 경우 소스 노드와 목적지 노드는 해당 노드의 경로를 통과시키지 않고 보안상 안전하다고 판단되는 노드를 통한 경로를 새로 구축하여 데이터 전송을 수행한다.

Y. Hu, D. B. Johnson, A. Perrig 등이 제안한 Ariadne은 DSR(Dynamic Source Routing)을 기반으로 하기 때문에 DSR에서 발생할 수 있는 다양한 공격에 대한 보안 방법을 제시하고 있다[3]. Ariadne의 기본적인 아이디어는 점 대점 인증에서는 MAC와 공유키를 사용하고 Broadcast 인증에는 TELSA 방식을 사용한다는 것이다. 즉, 경로 탐색에는 소스 노드가 목적지 노드와의 사이에 공유된 비밀 키를 이용하여 인증 값을 생성하고 RREQ에 포함시켜 전송하면 목적지 노드가 RREQ를 인증하고 RREP가 목적지 노드에서 소스 노드까지의 경로를 통해 소스노드에 전달되면 소스 노드가 다시 인증을 하는 방식이다. 또한 소스 노드와 목적지 노드 사이의 중간 노드들은 이전에 포함된 노드의 리스트에 수정을 가할 수 없도록 함으로써 설정된 경로에 대한 보안을 유지하는 기법이다.

Secure Ad hoc On-Demand Vector 기법은 가장 대표적인 애드 혹 네트워크의 보안 라우팅 기법이다.[4] 이 기법은 RREQ와 RREP를 인증하기 위하여 전자 서명을 사용하고, 홉 수를 인증하기 위하여 해쉬 체인을 사용한다. 네트워크의 노드들은 전자 서명으로 AODV 라우팅 패킷을 인증한다. RREQ나 RREP를 전달하고자 하는 노드는 임의의 숫자인 Seed값을 생성하고 네트워크 크기에 기초하여 최대 홉 수를 TTL(Time to Live)값으로 설정, 최대 홉 수 +1 길이의 One way Hash Function을 만든 후 Seed값을 해쉬 함수를 통해 변환시킨다. 이렇게 구성된 RREQ가 전달되면 이 패킷을 받은 노드는 먼저 RREQ 패킷이 타당한지 확인하기 위하여 전자 서명을 인증한다. RREQ 패킷이 목적지 노드에 도착하면 목적지 노드는 RREQ의 전자 서명을 통하여 인증 값을 검사한다. 인증 절차를 통과할 경우 해당 패킷을 보낸 노드에게 RREQ와 동일한 절차를 거친 RREP를 전송한다. RREP를 수신한 중간 노드는 전자 서명 값을 검사하고, 서명이 타당하면 RREP를 송신한 노드를 자신의 다음 경로로 인증하고 RREP를 재전송한다.

이러한 기존의 보안 라우팅 기법은 모든 보안 정보를 노드 자신이 직접 저장하기 때문에 공격자가 노드에 침입하여 보안 정보를 알아낼 경우 해당 보안 정보를 바탕으로 네트워크에 잠입하여 데이터 패킷을 가로채는 등의 보안에 대한 위험성이 나타날 수 있다.

또한, 최근에는 앞서 언급된 보안성과 관련된 문제를 해결하기 위해서 다양한 비밀 공유 기법을 응용한 라우팅 프로토콜 등이 제안되고 있다[12][13].

2.2 Token Escrow 기법

기존 애드 혹 네트워크의 보안 기법은 자신의 Key 값이나 Seed 값, 서명 값 등과 같은 보안 정보를 모두 직접 저장하고 있다가 서로 간 인증을 통해 네트워크를 구성하였다. 때문에 노드 자신이 직접 공격을 받아 보안정보를 강탈당할 경우에는 마땅한 해결책이 없었다. Token Escrow 기법은 이러한 문제를 해결하기 위해 자신의 보안 정보를 직접 저장하지 않고 다수의 제 3자에게 분배한 후 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].

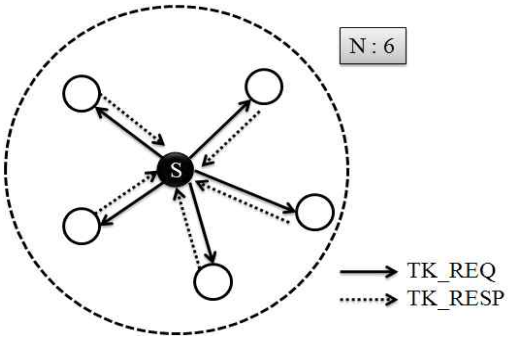

Fig. 1. Message Handshake for Constructing TES

SRPTES 기법의 동작방식을 보면, 우선 네트워크 구성 초기단계를 통해 각각의 노드들은 모니터링을 통해 검증된 자신의 이웃노드들과 Token Escrow Set (TES)라고 정의된 자신의 보안 정보를 분배할 집단을 구성한다.

TES 구성이 완료된 후 각각의 노드는 해쉬 함수를 통해 변환시킬 자신의 Seed값을 생성하고 Threshold Secret Sharing 기법[10]을 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 구성하게 된다.

하지만 이러한 SRPTES 기법을 사용한 라우팅 프로토콜에는 몇몇 문제가 발생하게 된다. 먼저 Secret Sharing 기법의 특성 상, T(Threshold)값이 작게 설정이 되어 있는 경우 공격자가 T개 노드에 대한 공격이 성공하여 Group Secret Key와 같은 보안 정보를 강탈당할 확률이 높아지게 된다. 또는 T의 크기가 TES의 멤버 수(N)와 비슷한 크기의 설정으로 구성시 몇몇 노드의 이동이나 특정 노드의 에너지 고갈로 인한 Token의 상실로 인해 초기의 Seed값을 제대로 복구해 낼 수 없다. 더욱이 N 값은 고정적이기 때문에 밀도가 높은 지역에서는 TES에 포함되지 못하는 노드가 생길 수 있으며 반대로 밀도가 낮은 지역에서는 N개의 노드를 채우지 못하여 TES 구성 자체가 불가능해 지는 문제가 발생할 수 있다.

3. 제안 기법

3.1 Token Escrow Tree

1) Token Escrow Tree 구성

본 논문에서는 앞서 언급한 기존 SRPTES 기법의 단점들을 보안하고자 2-level Tree 구조를 적용하여 TES를 구성하고자 한다. 즉, 해당 범위 내의 노드들끼리 Tree를 구성하여 초기 구성노드와 중간 노드들에게는 무작위 값을 저장시키고 Leaf 노드들에게만 보안 정보를 분배하여 공격자가 Token Escrow Tree의 구조를 파악하지 못하는 한 해당 그룹의 보안 정보의 안전을 최대한 보장해주는 것이 목적이다. 또한 TES의 크기를 고정적으로 설정하지 않고 각 구역별로 Tree 구조로 노드를 귀속시켜서 노드의 분포 밀도에 따라 TES에 속하지 못하는 노드가 생기거나, TES 구성이 되지 않는 구역이 발생하는 경우를 방지하게 할 것이다.

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

Step 1. 초기 구성 노드는 TES을 구성하기 위해서 Fig. 2과 같이 6개의 방향으로 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 Fig. 2와 같이 각각의 Queue를 생성한다.

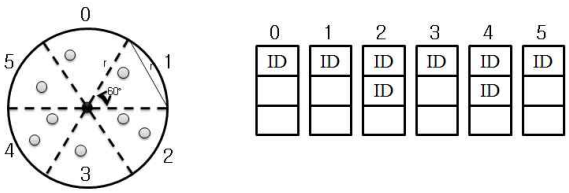

Fig. 2. Construction of 6 Way Queue Table

Step 4. Tree 구성 노드는 각각의 Queue Table에서 가장 먼저 도착한 노드를 자신의 Child 노드로 선정하고 해당 Queue Table의 나머지 정보를 Child 노드에게 전송한다.

Step 5. Fig. 3에서 볼 수 있듯이 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 전송한다. 끝으로 Parent 노드는 초기 구성노드에게 Tree가 완성됨을 알리는 메시지를 보낸다.

만약, Queue Table에 저장된 노드의 ID가 한 개인 경우, 해당 노드는 Fig. 4에서 나타나 있듯이 그 구역의 Leaf 노

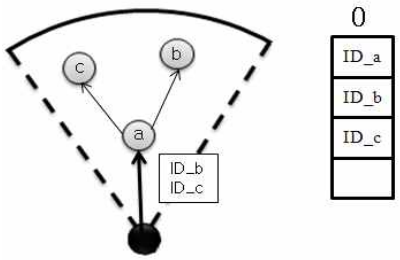

Fig. 3. Construct Tree using Queue Table

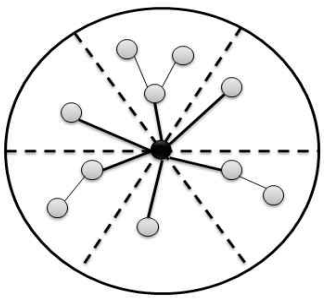

Fig. 4. Complete Token Escrow Tree

드로 동작한다. 또한, Tree의 깊이(Depth)를 2로 제한하여 트리 구성에 대한 과도한 자원 낭비를 줄이고자 하였다. 여섯 방향의 모든 구역에 대해 Tree가 완성된 후 보안 정보 분산 작업을 위해 Tree의 Root 노드는 Child 노드에게 해당 Tree의 Leaf 노드의 개수를 알려주어 Tree 구성 노드 모두가 Leaf 노드의 개수를 알게 한다. 이를 통해 Tree에 속한 모든 노드들은 (식 1)에 나타난 과정을 통해서 Leaf 노드의 개수에 따라 자신의 보안 정보를 Token 단위로 나누고 해당 Token은 Tree 구조를 따라 각각의 Leaf 노드들에게 하나씩 저장이 된다. (식 1)에서 L은 Tree를 구성하는 Leaf 노드의 수, n은 Token(Tk)을 나누기 위한 임의의 변수이지만 Threshold Secret Sharing 기법에 따라 L보다 커야한다. 각각의 나누어진 Token(Tki)은 TTL(Time to Live) 값을 가지고 있으며, 각 노드들 간 모니터링을 통해 이상이 없을 경우 TTL 값은 증가하며 이를 통해 Token 구성 단계의 횟수를 점차 줄어들 수 있다.

$$Tk = \sum_{i=1}^{L} Tk_i \,(\mathrm{mod}\, n) \qquad (1)$$

2) 경로 설정을 위한 Hash Function 적용

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 Fig. 5에서 볼 수 있듯이, 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 저장하게 된다.

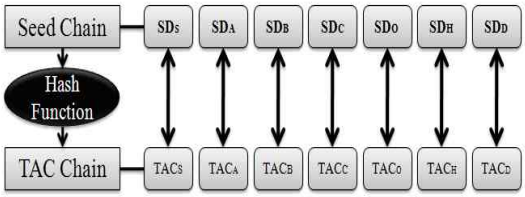

Fig. 5. Comparre between Seed Chain and TAC Chain

이후 목적지 노드는 Fig. 5과 같이 데이터 패킷을 통해 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 판단할 수 있고, 만약 내용이 다르게 나타난다면 중간 경로에 악의적인 노드가 존재할 수 있다는 판단을 내릴 수 있으므로 해당 경로를 사용하지 않고 네트워크 전체에 악의적인 노드가 존재한다는 경고 메시지를 발송, 주변 노드에 대해 모니터링하여 악의적인 노드를 찾아낼 수 있도록 한다.

3.2 Multipath Routing Protocol

기존에 무선 애드 혹 네트워크에서 사용되던 AODV와 같은 기법들은 홉 수가 적은 최단 경로를 선택하여 라우팅 경로를 설정하는 경향이 있다. 하지만 이러한 경로 설정은 악의적인 노드가 정상적 노드인 것처럼 위장하고 있다가 데이터 패킷을 강탈하거나 Dropping 공격을 수행하는 경우 데이터 패킷의 전송이 정상적으로 이루어지지 않아서 처음부터 다시 경로를 설정해야 하는 문제가 생긴다. 이를 방지하기 위하여 본 논문에서는 다중 경로를 통해 데이터 패킷이 정상적으로 전송되지 않는 경우 차선의 경로를 선택하여 전송함으로써 데이터 패킷의 지연 시간을 최대한 줄이고 각 노드의 에너지를 최대한 효율적으로 사용하고자 하였다.

1) Tree Security Level 설정

보안성을 지닌 다중 경로를 설정하는 기준은 홉 수와 해

당 경로의 보안 레벨을 기반으로 한다. 이를 위해서 각 노드들은 자신의 보안 레벨을 결정하여야 한다. 본 논문에서는 다중 경로를 지원하기 위한 보안 레벨을 Token Escrow Tree의 Leaf 노드의 개수로 설정할 것을 제안한다. 즉 많은 수의 노드로부터 인증을 받은 노드는 적은 수의 노드로부터 인증을 받은 노드보다 보안 레벨이 더 높게 설정된다. Fig. 6는 밀도가 높은 지역의 Tree의 보안 레벨이 상대적으로 적은 수의 노드가 이루는 Tree의 보안 레벨보다 높게 설정되는 것을 보여준다.

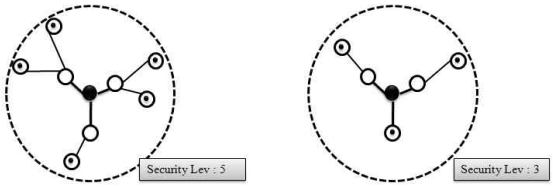

Fig. 6. Setting Security Level depend on Node Numbers

2) Security Level 기반의 Multipath Routing

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 레벨만을 고려한 가장 높은 보안성을 보장하는 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 (식 2)와 같은 계산을 통해 경로를 선택한다.

$$P = \mathrm{argmax}_{i \in R}[(1-\alpha) \times \frac{E(SL_i)}{\delta(SL_i)} + \alpha \times \frac{1}{Hopcount}] \quad (2)$$

(식 2)에서 R은 RREQ가 전달된 경로의 노드 집합을 나타내고 E(SLi)는 해당 경로의 각 노드에 대한 보안 레벨들이 가진 값들의 평균이고, 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 Hopcount는 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 (식 3)과 같이 구성되며 이러한 식은 보안 레벨이 가장 높은 경로인 ③번 경로를 결정하는 수식이 된다.

$$P = \mathrm{argmax}_{i \in R}[\frac{E(SL_i)}{\delta(SL_i)}] \quad (3)$$

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 (식 3)을 통해 계산된 보안 레벨이 가장 높은 노드를 연결한 경로로 데이터 패킷을 전송한다.

그리고 악의적인 노드에 의한 데이터 Dropping 공격을 방지하기 위해 일정 시간이 지난 후에도 목적지 노드에 데이터 패킷이 전송되지 않을 경우 Fig. 7처럼 목적지 노드는 세 개의 경로 모두를 통해 데이터 패킷을 받지 못했다는 것을 알리는 에러 메시지 DERR을 전송한다. DERR 메시지를 전송받은 소스 노드는 자신이 데이터 패킷을 전송했던 경로보다 보안성이 한 단계 높은 경로를 통하여 데이터 패킷을 전송하고 기존의 데이터 패킷을 전송한 경로를 파기한다.

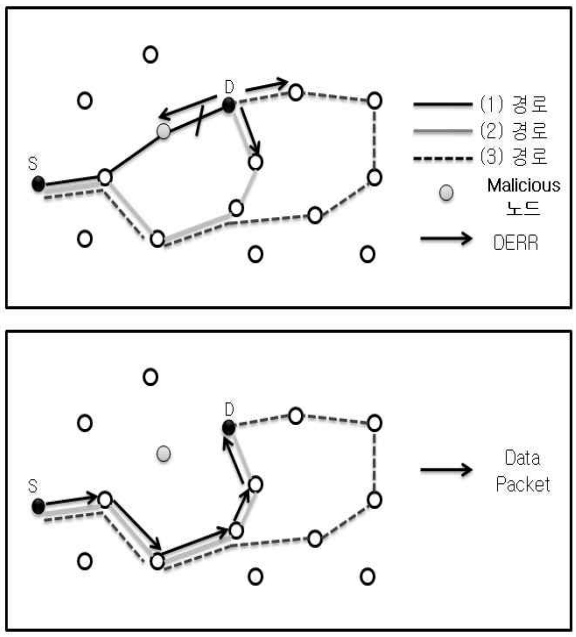

Fig. 7. Request Repeat Process of DERR and Data Packet

4. 시뮬레이션

4장에서는 GloMoSim 2.03 시뮬레이터를 이용하여 본 논문에서 제안하는 기법의 성능을 평가해 본다. 무선 애드 혹 네트워크의 시뮬레이션은 GloMoSim Ver 2.03의 AODV소스를 기반으로 사용하였고, 제안 기법은 그 소스를 수정하여 실험하였다.

4.1 성능 평가 모델

Table 1. Mobile Ad-Hoc Networks Environment for Simulation

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
Mobility Model	Random Waypoint
α Value	0, 0.5, 1

Table 2. Simulation Field Environment

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

각 무선 애드 혹 노드의 전력은 미리 동일하게 설정하였다. 모든 노드의 초기 전력은 10 J로 설정하였고, 송신할 때의 전력 소모를 30 mW로 수신할 때의 전력 소모를 10 mW로 설정하였다. 성능 평가를 하는 환경은 가로 1500 m, 세로 1500 m의 공간에 노드가 임의로 분포되어 있는 환경으로 설정하였고, 총 노드의 수는 각각의 실험에 맞게 50개부터 400개 까지 다양하게 설정하였다. 전체 노드 수 대비 악의적인 노드의 비율은 10%로 제한하고 성능 평가를 수행한 시간은 100 초 단위로 설정하였다. 그리고 각 노드의 에너지 잔량이 초기 에너지 잔량의 10% 미만으로 남을 경우에는 해당 노드의 기능이 정지된다고 가정하였다. 성능 평가는 제안하는 알고리즘의 성능을 비교하기 위해서 Secure AODV와 SRPTES를 같은 조건에서 수행하여 비교 대상으로 고려하였고, 각 실험은 시뮬레이션을 15 번씩 반복 수행하여 그 평균값을 사용하였다.

각 실험의 평가 기준은 다음과 같다. 네트워크를 구성하는 전체 노드의 수가 50개 단위로 증가함에 따라 해당 네트워크의 패킷 전송 성공률을 비교하였고, 10% 이하의 에너지를 가진 노드는 네트워크에서 배제함으로써 생존 노드의 수를 통해 전체 네트워크의 평균 생존 시간을 살펴보았으며, 노드의 수에 따른 네트워크의 평균 라우팅 오버 헤드의 양을 비교하여 각 기법의 성능을 비교 측정하였다.

4.2 노드 수에 따른 패킷 전송 성공률

본 논문은 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.

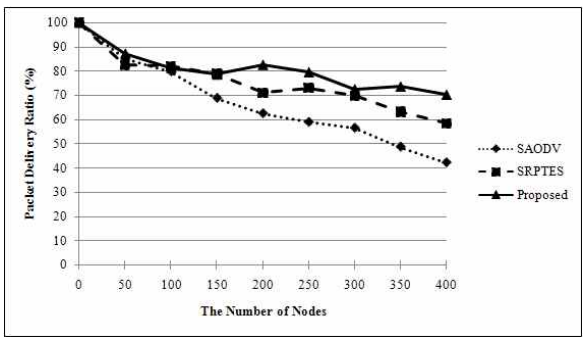

Fig. 8. Packet Sucess Ratio depend on Node Numbers

Fig. 8에서 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. 또한 악의적인 노드의 Dropping 공격에 대해서도 다중 경로의 우회 전송을 통하여 피해 이후의 빠른 재전송을 고려하였기 때문에 대체적으로 비교 기법보다 높은 전송 성공률이 나오는 것을 확인할 수 있었다.

4.3 네트워크의 평균 생존 시간

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.

Fig. 9을 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. 제안하는 알고리즘의 경우 다른 두 기법들보다는 일정 에너지 잔여량 이하로 내려가는 노드의 수가 적고, 생존 노드의 비율이 50% 이하가 되기까지 약 930초 정도의 시간

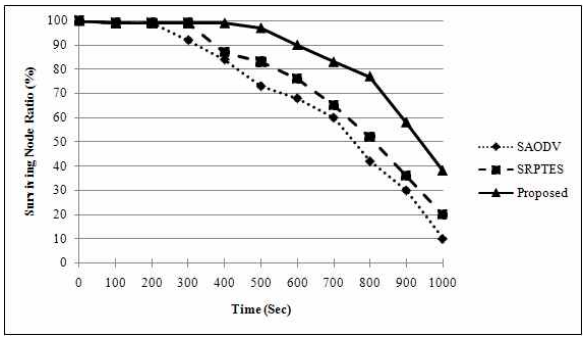

Fig. 9. Average Life time of Entire Networks

이 걸리는 것을 보아 전체 네트워크의 생존 시간이 길게 유지되는 것을 보여준다.

즉, 제안기법은 악의적인 노드로부터 보안 정보를 지키기 위해 Token Escrow Tree를 사용함으로써 최대한 보안 정보를 감추고 또한 다중 경로를 지원하여 악의적인 노드가 정상 노드인 척 잠복해 있다가 Dropping 공격을 수행하는 경우나 정상 노드가 악의적인 노드로 변절하는 경우 차선의 경로로 데이터 패킷을 전송함으로써 경로의 재설정을 위한 패킷의 전송을 최대한 줄이게 되어 네트워크를 구성하는 각 노드의 에너지 소모를 최소화하였기 때문에 기존의 두 기법에 비해서 향상된 성능을 보인다.

4.4 노드 수에 따른 평균 라우팅 오버헤드

오버 헤드의 측정은 노드의 수에 따라 평균적으로 라우팅에서 발생하는 메시지 전달 횟수로 측정하였으며 해당 실험에서는 각 네트워크의 노드 수에 비례하여 임의의 10% 노드는 악의적인 노드로 동작하게 하였다.

Fig. 10에서 x 축은 50개부터 400개 까지 각각 네트워크를 구성하는 전체 노드의 수를 나타내며 y 축은 라우팅 오버 헤드를 나타내는데 각각의 기법에서 라우팅을 위하여 전달되는 평균적인 메시지 전달 횟수를 측정하여 기록하였다. 본 논문에서 제안하는 알고리즘은 Tree를 구성하는 과정에서의 메시지 전달과정 때문에 약간의 오버 헤드가 더 발생한다.

하지만 이는 경로의 재설정을 위한 경로 탐색의 과정에서 나오는 메시지 전달 횟수에 비하면 크지 않고, 다중 경로를 설정하였기 때문에 경로 탐색을 다시 해야 되는 경우를 최대한 줄임으로써 평균 오버 헤드를 안정적으로 유지할 수 있는 것을 살펴볼 수 있다.

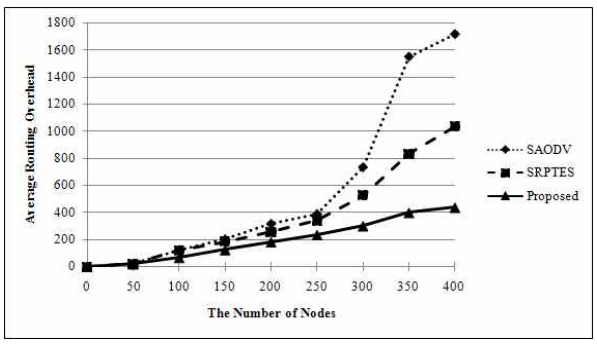

Fig. 10. Average Routing Overhead Depend on Node Numbers

5. 결 론

기존 애드 혹 네트워크의 보안 라우팅 알고리즘에서는 자신의 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 과정에서 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 보안 정보 분배를 위한 Tree를 구성하여 보안 정보들을 나누어 저장시키고, 동시에 Leaf 노드의 개수에 따라 Tree의 보안 레벨을 설정하여 보안 레벨을 고려한 다중 경로를 유지할 수 있도록 한다. 이를 통해 네트워크 전체 노드의 보안 정보를 안전하게 보관하고 경로를 다시 구축하는데 소모되는 에너지를 최소화하고 전체 네트워크의 경로 구성을 위한 오버 헤드 역시 최소화 할 수 있었다.

참 고 문 헌

[1] G. Peng and Z. Chunanyun, “Routing Attacks and Solutions in Mobile Ad hoc Networks,” Proceedings 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,” Proceedings 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,” Proceedings 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.
[8] H. L. Nguyen and U. T. Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," Proceedings of IEEE ICNICONSMCL'06, pp.149-154, Apr., 2006.
[9] P. G. Argyroundis and D. O'Mahony, "Secure routing for mobile ad hoc networks," Journal of IEEE Communications Surveys & Tutorials, Vol.7, pp.2-21, Third Quarter 2005.
[10] A. Shamir, "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979.
[11] D. Carman, P. Kruus and B. Matt, "Constraints and approaches for distributed sensor network security". Technical Report 00-010, NAI Labs, 2000.
[12] Chen. Siguang and Wu. Meng, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks", Journal of Systems Engineering and Electronics, Vol.22, No.3, pp.519 - 527, June, 2011.
[13] Meng. Xianyong and Li. Yangmin, "A novel verifiable threshold signature scheme based on bilinear pairing in mobile Ad Hoc Network", Information and Automation (ICIA), 2012 International Conference on, pp.361-355, June, 2012.

이 재 식

e-mail : ljsljslove@naver.com
2008년 서강대학교 컴퓨터학과(학사)
2010년 서강대학교 컴퓨터공학과 공학석사
관심분야 : 무선통신망, 센서네트워크 등

김 성 천

e-mail : ksc@sogang.ac.kr
1975년 서울대학교 공과대학 공업교육학 (전기전공)학사
1979년 Wayne State Univ. 컴퓨터공학 (공학석사)
1982년 Wayne State Univ. 컴퓨터공학 (공학박사)
1982년～1984년 캘리포니아주립대 조교수
1984년～1985년 금성반도체(주) 책임연구원
1985년～현 재 서강대학교 컴퓨터학과 교수
관심분야 : 병렬처리시스템(Parallel Computer Architecture, Interconnection Network), WDM technology를 이용한 cluster system, 유비쿼터스 컴퓨팅, Pervasive Computing