Ad Hoc 네트워크 라우팅 보안을 위한 다중경로 기반의 MP-SAR 프로토콜

정회원 한 인 성*, 유 황 빈*

Multiple Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network

In-sung Han*, Hwang-bin Ryou* ***Regular Members***

요 약

기존의 SAR(Security Aware Routing)[9] 프로토콜은 Ad Hoc 네트워크의 보안경로를 발견하는 프로토콜로, 이동 노드에 부여된 보안레벨 속성 값을 라우팅 정보로 이용하는 보안라우팅 프로토콜이다. 그러나 SAR 프로토콜은 암호화된 데이터 전달을 위해 보안노드를 경유로 데이터를 전송하므로 비밀통신과 효율적인 통신이 고려되지 않고 있다. 또한, AODV[3] 프로토콜 기반으로 동작하기 때문에 데이터의 전송 중 중간노드의 배터리소진 또는 중간노드의 이동으로 데이터 전달에 있어 통신이 단절될 경우 보안노드를 경유하는 라우팅 경로를 재탐색하게 되어 데이터의 전송지연 문제가 발생한다. 그 외에도 SAR 프로토콜의 특성상 재탐색의 경우 노드간의 연결은 가능하지만 데이터 전송에 있어서 요구되는 노드의 보안레벨 이하의 노드인 경우 경로설정이 중단되는 문제들로 재연결이 용이하지 않다. 본 논문에서는 SAR 프로토콜의 문제점을 개선하기 위해 다중경로 기반의 SAR 프로토콜인 MP-SAR을 제안한다. MP-SAR은 데이터의 기밀성을 유지하기 위해 SAR의 보안경로 탐지기법의 확장으로 다중경로를 탐색하고, 유효한 최단보안경로의 이용으로 안전한 고속의 데이터 전달을 할 수 있다.

Key Words : Ad-hoc networks, MANET, Secure routing, SAR, ADMDV

ABSTRACT

As pervious the SAR(Security Aware Routing)[10] protocol is an secure Ad Hoc network protocol that finds a secure path, it is the security routing protocol that uses the security level of nodes as the routing information. However, the SAR protocol sometimes transfers data through inefficient transmission paths because it always tries to find secure nodes for a safe transmission. Since it is a protocol based on AODV[6], it will cause transmission delay as researching of security routing path. when a node is out of the data transmission range as its battery dying or movement. Although it is possible to connection of nodes because a characteristic of the SAR protocol, the connection is not easy to reconnect when the security level of intermediate node is lower than the level requested by a source node. In this paper, we suggest the MP-SAR based on the SAR to solve the SAR protocol's problem. The MP-SAR seeks multiple secure path for maintenance of data confidentiality using the expanded secure path detection techniques based on the SAR . It can transfer data quickly and reliably by using the shortest efficient path among multiple paths. In the research result, we proved a outstanding perfomance of MP-SAR than the previous SAR through comparison and analysis.

* 광운대학교 컴퓨터과학과 (ishan78@kw.ac.kr)
논문번호 : KICS2007-12-559, 접수일자 : 2007년 12월 25일, 최종논문접수일자 : 2008년 5월 7일

Ⅰ. 서 론

이동 Ad Hoc 네트워크는 이동성을 가진 다수의 노드들에 의해 자율적으로 구성되는 임시적인 네트워크로서, 기반 망이 존재하지 않거나 기반 망에 기초한 네트워크의 전개가 용이하지 않은 지역에서 임시적으로 네트워크를 구성하기 위한 목적으로 연구되어 왔다. 이동 Ad Hoc 네트워크를 구성하는 노드들은 무선 인터페이스를 가지며, 이동 컴퓨팅 기능을 가진 호스트와 라우팅 기능을 가진 라우터를 동시에 만족하는 형상으로 흔히 이동 노드로 불려진다. 이러한 이동 노드는 전파 도달 거리가 제한되므로 중간 노드로서 데이터 전달 기능을 가지며, 배터리를 사용하므로 에너지의 공급이 일정치 않은 특성을 갖는다[1,4,6].

최근 들어, 이동 Ad Hoc 네트워크 기술은 홈 네트워킹, 센서 네트워크, PAN(Personal Area Net-work) 등 다양한 응용 분야로의 적용이 예상되고 있으며 차세대 네트워킹 방식의 하나로서 활발한 연구가 진행되어 실용화단계에 있다. 따라서 이동 Ad Hoc 네트워크 라우팅 프로토콜은 Ad Hoc 네트워크 구성 노드들 간의 통신을 가능하게 하는 기술로서 Ad Hoc 네트워크의 가장 중요한 연구 분야로 자리 매김하고 있다[4,8].

그러나, 이동 Ad Hoc 네트워크 환경은 무선 인터페이스를 사용하기 때문에 기존 유선 네트워크에 비해 더욱 많은 위험에 노출되어 있다[5,10]. 기본적인 Ad Hoc 네트워크의 보안 요구조건은 다른 통신 네트워크에서 요구되는 것과 동일하지만, 이동 Ad Hoc 네트워크에서는 Multiple Hop 방식에 의해 라우팅을 수행할 경우 악의적인 중간노드로 부터 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 특히, 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로, 암호 키에 크게 의존하게 된다. 또한, 이동 Ad Hoc 네트워크 환경은 모든 노드들이 분산되어 있고, 어떠한 고정된 기반구조도 없으며, 모든 노드가 공평하게 역할을 나누어 갖는다는 특징을 갖는다. 이와 같은 많은 위험에 노출되어있는 Ad Hoc 네트워크 환경에서 라우팅 설정상의 보안문제를 해결하기 위해 제안된 경로설정 기법 중의 하나가 SAR 프로토콜 기술이다[9].

SAR 프로토콜은 Ad hoc 환경에서 안전한 라우팅 경로를 탐색하는 프로토콜로써, 노드가 갖고 있는 보안레벨 속성 값을 이용해 출발지 노드에서 요구한 보안레벨 이상의 노드만을 경유할 수 있도록 보안경로탐색이 가능하도록 한 라우팅 프로토콜이다. 그러나 SAR 프로토콜은 보안노드만을 통해 데이터를 전송하기 때문에 비효율적인 데이터 전송경로를 갖게 되며, AODV 프로토콜을 기반으로 하기 때문에 데이터의 전송 중 중간노드의 배터리소진 또는 중간노드의 이동으로 데이터 전달 범위를 벗어날 경우 보안 라우팅 경로를 처음부터 재탐색하게 되어 전송시간 지연 문제가 발생한다. 그 외에도 SAR 프로토콜의 특성상 재탐색의 경우 노드간의 연결은 가능하지만 데이터 전송노드가 요구한 노드의 보안레벨 이하의 노드인 경우 경로설정이 중단되는 문제점이 있어 재 연결이 용이하지 않다.

본 논문에서는 SAR 프로토콜의 문제점을 개선하기 위해 다중경로 기반의 SAR 프로토콜인 MP-SAR을 제안한다. MP-SAR은 데이터의 기밀성을 유지하기 위해 SAR의 보안경로 탐지기법을 확장하여 다중경로를 탐색하고, 이 중 유효한 최단경로를 이용해 빠르고 신뢰성 있는 데이터 전달을 할 수 있다. 기존의 SAR 프로토콜과 MP-SAR 프로토콜의 성능을 비교분석함으로서 MP-SAR의 성능을 보인다.

본 논문의 Ⅱ장에서는 제안기법과 관련된 기술들에 대한 설명을 하였고, Ⅲ장에서는 제안기법을 위한 라우팅 테이블의 구조와 동작과정에 대해 설명하였다. Ⅳ장에서는 MP-SAR과 SAR의 실험성능을 비교 분석하였으며 Ⅴ장에서 본 논문의 결론을 기술하였다.

Ⅱ. 관련연구

2.1 SAR 프로토콜

SAR 프로토콜은 AODV 기반의 보안라우팅 프로토콜로, 각기 다른 Ad-hoc 노드의 보안속성을 이용해 안전한 보안경로를 설정한다. 즉, SAR은 기존의 라우팅 메트릭을 Ad-hoc 노드의 보안레벨로 이용함으로써 Ad-hoc 노드간의 신뢰관계를 형성하며 정확하게 보안 값을 표현할 수 있는 특징이 있다.

그림 1의 시나리오는 전장에서 두 General 노드가 SAR 라우팅 프로토콜을 이용해 경로설정이 이루어지는 과정을 보이고 있다. 발견된 전송 경로에서 두 General 노드 사이에 General 노드보다 보안레벨이 낮은 Private 노드를 발견하게 될 경우 해당 경로를 취소하고, 두 General 노드는 최소한의 신뢰가 가능한 Officer 노드들을 통해 데이터를 교환한다. 잠재적인 위험성이 존재할 수 있는 노드를 이용

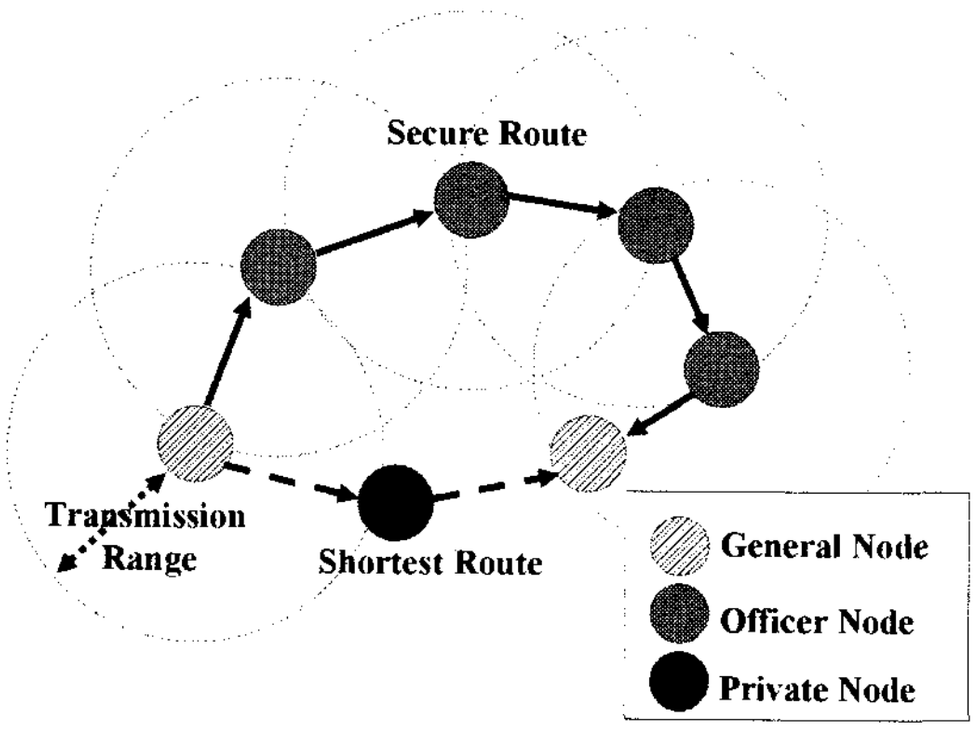


그림 1. SAR 라우팅 동작과정

해 전달되는 정보들은 신뢰할 수 없는 노드에 의해 정보의 유출 또는 훼손으로 임무수행을 위험에 처하게 할 수 있는 가정을 한 것이다.

두 General 노드는 SAR을 이용함으로서 이러한 잠재적인 문제를 유발할 수 있는 주변 노드를 배제한 경로를 구성한 것이다. 데이터를 전송하는 General 노드의 경로탐색 프로토콜은 경로 협상을 위한 메트릭으로, 네트워크 구성 노드들의 보안레벨 속성을 포함하고 있으며 이러한 정보를 통해 Private 노드와의 경로설정을 회피할 수 있다. 만약 경로탐색 프로토콜이 경로를 발견할 수 있다면, [그림 1]과 같이 두 General 노드들은 Officer 노드들을 경유하는 라우팅 경로를 구성할 수 있다.

2.2 AOMDV

AOMDV(Ad hoc On-demand Multipath Distance Vector)[8] Routing Mechanism 는 루프가 없고 링크 비겹침 경로들을 계산하기 위해 AODV를 확장한 다중경로 라우팅 프로토콜이다. 다중경로들을 유지하기 위하여 각 목적지를 위한 라우팅 경로들은 해당 홉 카운트를 가진 다음 홉들의 리스트를 포함하게 된다. 다음 홉들은 동일한 시퀀스 번호를 갖으며, 각 목적지 노드에 대하여 중간노드들은 모든 경로에 대해 최대 홉 카운트로 정의되어 광고된 홉 카운트를 유지하게 된다. 이것은 목적지 노드를 찾기 위한 루트 탐색 메시지에 사용된다. 중간노드에 의해 수신된 각각의 중복된 루트 광고는 목적지 노드의 대체 경로를 정의한다.

루프 방지를 보장하기 위하여 노드는 목적지에 대한 광고된 홉 카운트보다 적은 홉을 가지고 있는 경우에만 목적지에 대한 대체 경로를 수용하게 된다. 만약 최대 홉 카운트가 사용된다면, 광고된 홉 카운트는 같은 시퀀스 번호에 대하여 변경되지 않는다. 보다 큰 시퀀스 번호를 가진 루트 광고를 받게 되는 경우 다음 홉 리스트와 광고된 홉 카운트는 재 초기화된다.

루프 방지를 보장하기 위하여 노드는 목적지에 대한 광고된 홉 카운트보다 적은 홉을 가지고 있는 경우에만 목적지에 대한 대체 경로를 수용하게 된다. 만약 최대 홉 카운트가 사용된다면, 광고된 홉 카운트는 같은 시퀀스 번호에 대하여 변경되지 않는다. 보다 큰 시퀀스 번호를 가진 루트 광고를 받게 되는 경우 다음 홉 리스트와 광고된 홉 카운트는 재 초기화된다.

AOMDV는 노드 비겹침 또는 링크 비겹침 경로를 찾는데 사용될 수 있다. 노드 비겹침 경로들을 찾기 위하여 각 노드는 중복된 RREQ(Route Request)들을 즉시 거절하지 않는다. 출발지 노드의 다른 이웃노드들로부터 수신된 각각의 RREQ는 노드 비겹침 경로를 정의한다. 노드들은 중복된 RREQ들을 브르드캐스트 할 수 없기 때문에 목적지 노드의 다른 이웃에서 전송된 중간노드에 도착하나 두 개의 RREQ는 같은 노드를 다시 전송하지 않게 된다. 다수의 링크 비겹침 경로를 구하기 위하여 목적지는 첫 번째 홉에 상관 없이 중복된 RREQ들을 전송하게 된다. RREP(Route Reply)의 첫 번째 홉에서 링크 비 겹침성을 보장하기 위하여 목적지는 유일한 이웃들로부터 도착하는 RREQ들에 대하여서만 반응하게 된다. 첫 번째 홉 이후에, RREP들은 노드 비겹침과 링크 비겹침인 역방향 경로들을 따라서 전송된다. 각 RREQ와 RREP의 전송 과정은 중간노드에서 만나게 될 수도 있으나, 링크 비겹침성을 보장하기 위하여 목적지로의 다른 역방향 경로를 선택한다. 본 논문에서 제안한 기법은 노드 최대한의 노드 비겹침을 기반으로 보안경로들과 다중경로들을 확보하여 신뢰성과 보안성 모두를 충족할 수 있는 동작을 수행한다.

Ⅲ. 제안기법

본 논문에서는 SAR 프로토콜의 문제점을 개선하기 위해 AOMDV 기반의 MP-SAR 보안경로탐색 기법을 제안한다. 2.1절에서 소개한바와 같이 기존의 SAR은 일정한 보안 수준 값을 갖는 보안노드만을 발견하기 때문에 단일 보안경로설정의 지연과 목적지 노드와의 연결이 어렵다. 이와 같은 문제점의 개선을 위해 그림 2와 같이 MP-SAR은 보안노

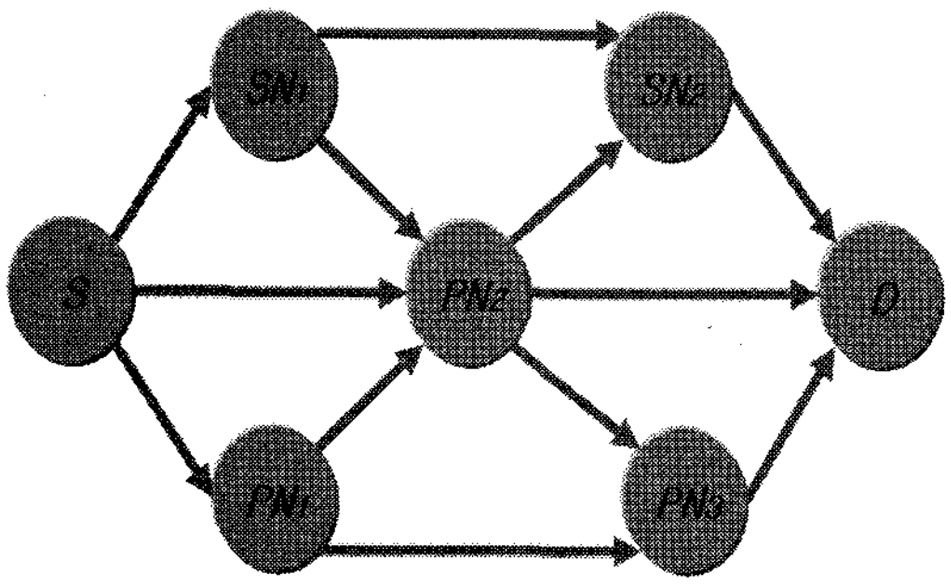


그림 2. 보안경로와 다중일반경로 발견

드들만으로 구성된 완전한 보안경로(S,SN1,SN2,D)와 일반노드를 경유하는 다중일반경로들을 발견한다.

보안경로의 주요한 목적은 다중경로들 중에서 가장 안전하고 빠른 데이터 전송 경로생성을 위해 출발지 노드와 목적지 노드사이에 보안요소와 인증정보 그리고 보안 전송경로에 필요한 세션 키를 교환하는 경로로 이용된다. 한편, 이용 중이던 최단경로가 손실될 경우 출발지 노드는 다중경로들 중 다음 최단경로를 선택하고 안전한 전송경로 설정을 위해 목적지 노드와 보안경로를 통해 동일한 세션 키를 재전송한다.

본 논문에서는 보안경로와 다중일반경로들의 발견을 위해 다음과 같이 몇 가지 가정을 한다. 첫 째, 다중경로 발견은 기본적으로 AOMDV 를 기반으로 하며, 모든 Ad Hoc 구성노드들은 UID(Unique Identifier)정보를 갖는다. 둘째, Ad Hoc 노드 A와 B 사이는 통신연결이 존재하며 상호 양방향 통신이 가능하다. 셋째, Ad Hoc 네트워크에 존재하는 모든 보안노드들은 보안레벨 속성이 정의되어 있다. 넷째, Ad-Hoc을 구성하는 보안노드들은 공개키와 개인키를 통해 상호간의 인증을 처리할 수 있다[10].

3.1 경로발견

제안된 MP-SAR에서 보안경로와 다중일반경로의 탐지과정의 핵심은 RREQ에 출발지 노드의 정보와 보안레벨을 추가 확장시켜, 목적지 노드가 미리 정해진 일정 시간(즉, 프로토콜 파라미터 중 1초의 RREQ 대기시간) 동안 도착한 다수의 RREQ들 중 보안경로와 다중일반경로를 수집하고 최적의 경로를 선택하는 것이다. 따라서 본 논문에서는 제안 프로토콜을 위해 출발지 노드의 정보와 보안정보를 처리하기 위해 AOMDV 라우팅 프로토콜을 확장하였다.

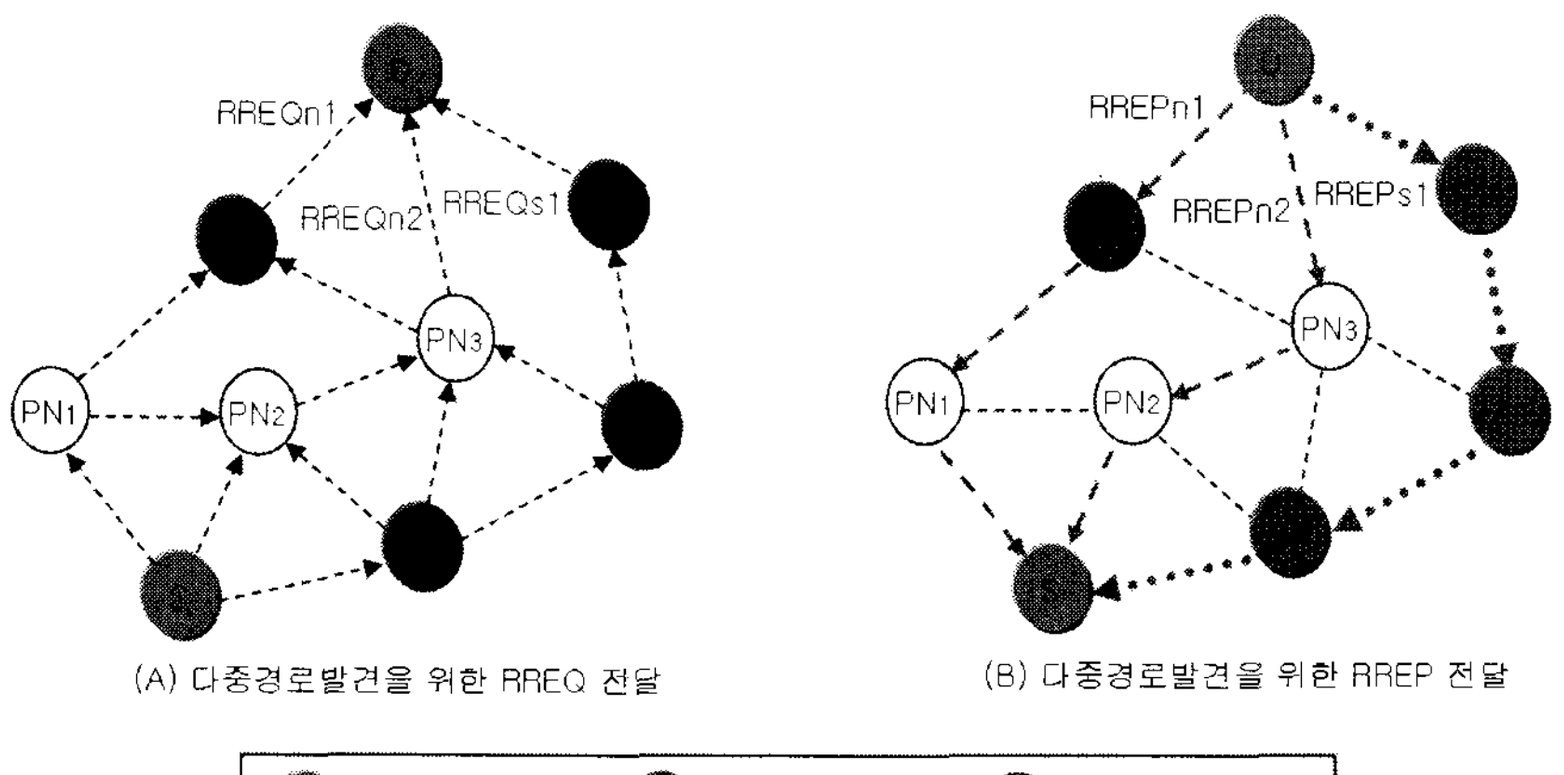
출발지 노드는 목적지 노드까지의 경로를 필요로 할 때, 출발지 노드 UID 정보와 요구 보안레벨 정보(보안경로 발견을 위해 필요로 하는 보안레벨)를 포함한 RREQ를 생성 후 이를 이웃 노드로 브로드캐스트 함으로써 보안경로와 다중일반경로 발견과정을 시작한다. 출발지 노드에서 브로드캐스트한 RREQ가 네트워크 전역에 플러딩 되기 때문에 한 노드는 동일한 브로드캐스트 ID를 갖는 여러 개의 같은 RREQ를 수신할 수 있다. 목적지 노드는 수신된 RREQ로부터 최대의 노드 비중첩 경로를 찾아내기 위해 수신된 다수의 RREQ로부터 경로정보를 확인한다. 이러한 경로정보를 위해 출발지 노드나 중간 노드에서 RREQ를 전송 시 요구 보안레벨과 출발지 라우팅 주소 정보로서 UID를 RREQ에 추가한다.

AODV를 기반으로 한 SAR에서는 처음 도착한 RREQ가 요구 보안레벨을 검증하고 역경로(Reverse Path)를 설정하는데 이용되므로, 중복으로 도착한 RREQ는 버리게 된다. 하지만 AOMDV를 기반으로 하는 MP-SAR에서는 중복 RREQ가 보안경로뿐만 아니라 다중일반경로를 설정할 수 있다. 중복된 모든 RREQ는 목적지 노드에서 잠재적인 보안경로와 대체경로를 찾기 위한 최적의 비중첩 노드 경로선택 알고리즘을 수행한다.

출발지 노드와 이웃한 중간노드는 RREQ를 수신하는 즉시 RREQ의 목적지 노드를 확인한다. 중간 노드는 자신의 라우팅 테이블에서 목적지가 일치하는 일반다중 라우팅 경로들과 보안정보를 확인하고 요구 보안레벨이 일치할 경우 역 경로 설정을 위한 RREP를 생성한다. 만약 중간노드에 RREQ의 목적지 노드와 일치하는 경로가 없을 경우, 중간노드는 RREQ의 라우팅 리스트에 중간노드의 정보를 추가하고 다음 이웃 노드로 전달하는 처리를 수행한다. 여기서 중간노드가 출발지 노드의 바로 이웃한 노드인 경우 중간 노드는 RREQ의 타입을 RREQs(보안경로 탐색을 위한 RREQ)로 변경할 지 여부를 판단한다. 중간 노드는 RREQ에 설정된 보안레벨과 자신의 보안레벨을 비교하여 보안레벨이 동일하거나 요구 보안레벨 이상일 경우 중간노드는 공개키와 자신의 개인키를 이용해 RREQ의 암호화된 필드를 복호화하여, 출발지 라우팅 리스트에 자신의 요구정보와 보안레벨을 추가한다. 요구 보안레벨보다 낮은 경우 중간 노드는 RREQ의 암호화 되지 않은 필드에 소스라우팅 정보를 추가하며 다시 이웃 노드들로 브로드캐스트 한다. 이때는 처음 도착한 RREQ만이 다시 브로드캐스트 된다. 목적지 노드는 수신된 RREQ를 확인해 가정하며, 먼저 도착한 RREQ

선택경로 알고리즘	1. 첫 번째 경로 $P_1 = \{M_S, M(1,1), M(1,2), ..., M(1,k-1), M_D\}$를 주경로로 사용 2. j번째 경로 $P_j = \{M_S, M(j,1), M(j,2), ..., M(j,k(i)-1), M_D\}$에 대하여, P_1와P_j의 중첩 노드 수 $V_j = \mid P_1 \cap P_j \mid$를 계산. $j = 2,3,...,n$ 3. 모든 j에 대하여 $V_{\min} < V_j$가 되도록 V_i의 최소값을 갖는 경로로 선택 4. $P2$에서 Pn까지의 n-1개 경로로부터 $V_{\min}$을 갖는 경로를 선택 5. 만약 $V_{\min}$!= 0이고 $V_{\min}$을 갖는 경로가 2개 이상이면, 그 중에서 중첩 링크의 수가 가장 적은 경로를 선택 6. 선택된 경로가 3개 이상인 경우, 그 중에서 가장 먼저 수신한 *RREQ*에 해당하는 경로를 선택

그림 3. 비중첩 노드 경로 선택 알고리즘



(A) 다중경로발견을 위한 RREQ 전달

(B) 다중경로발견을 위한 RREP 전달

그림 4. 보안경로와 다중경로 발견과정

를 다중경로들 중 그림 3과 같은 알고리즘을 이용해 최단 경로를 판단하고 이를 주요 데이터 전송경로로 결정한다.

목적지 노드는 자신의 수신 순서번호가 RREQ에 포함되어 있는 수신 순서 번호보다 크거나 같으면 중간 노드에서와 같은 방법으로 역 경로를 형성한다. 효율성과 저비용 구현을 위하여, 경로 설정 알고리즘은 처음 수신한 경로를 데이터 전송을 위한 주경로로 선택한 후 주경로와 비교해 최대의 노드 비중첩성을 갖는 대체경로를 찾는다. 표 1은 RREQ와 RREP를 이용한 MP-SAR의 경로발견 과정을 순서화된 동작과정으로 나타내고 있다.

그림 4는 제안 프로토콜의 보안경로와 다중일반경로 발견과정을 보이기 위한 Ad Hoc 네트워크 동작 구조이다. Ad Hoc 네트워크 노드의 구성으로써, 출발지 노드 S와 보안노드 SN1, SN2, SN3, SN4 및 일반노드 PN1, PN2, NN3으로 구성되어 있는 이동 Ad Hoc 네트워크 상황을 가정 한다. 처음 출발지 노드 S는 RREQ를 이웃노드 PN1, PN2, SN1으로 브로드캐스트 하고, 경로발견 과정은 위에서 나타낸 표 1과 같은 과정으로 동작한다. 목적지 노드는 RREQs가 도착하기 이전에 수신한 RREQ들과 RREQs들을 수신하며, 최초의 RREQs를 수신 후 1초 동안 n개의 RREQ를 수신 한다. 목적지 노드는 RREQs를 복호화 하고 자신이 목적지 노드임을 확인한다. 이후, 목적지 노드는 가장 처음 도착한 RREQn1을 다중경로들 중 주 경로로 선택하여 이를 기준으로 [그림 3]과 같은 비중첩 노드 경로 발견을 위한 알고리즘을 처리한다. 결정된 다중경로들은 RREQ들의 경로에 해당하는 RREP 생성 후 출발지 노드로 전송한다. 목적지 노드는 동시에 암호화된 전송 경로을 위한 세션 키를 생성하여 이를 RREQs의 역 경로로 RREPs에 포함시켜 출발지 노드로 전달한다.

표 1. MP-SAR 프로토콜 경로발견 동작과정

	출발지 노드	중간노드	목적지 노드
경로 발견 (RREQ)	1. 목적지 노드에 대한 유효한 보안경로와 일반경로가 존재하면, 자신의 보유 경로를 이용하고, 둘 중 하나라도 없을 경우 자신의 정보와 요구 보안레벨을 추가 후 전달	2. 목적지 노드의 요구보안레벨보다 크거나 같고, 유효한 보안경로와 일반경로가 존재하면, 출발지 노드로 RREP를 전달한다. 유효한 보안경로와 일반경로 둘 중 하나라도 없으면 자신의 정보를 RREQ에 추가하여 전달	3. 가장 처음 수신된 RREQ로부터 포함된 경로를 주경로로 선택하고, 보안 RREQ 수신을 대기. 보안 RREQ를 수신 후 미리 정해진 일정시간 동안 기다림. 주경로와 비교해 최대의 노드 비중첩성 경로를 대체경로로 설정
경로 발견 (RREP)	6. 보안경로와 주경로 그리고 대체경로를 통해 RREP를 받고, 라우팅 테이블을 갱신	5. RREP를 받은 후, 라우팅 테이블을 갱신하고 다시 출발지 노드로 RREP를 전송	4. 보안경로 및 주경로 그리고 대체경로를 통해 출발지 노드로 RREP를 전송

3.2 제안프로토콜의 라우팅 테이블

제안된 프로토콜을 위한 라우팅 테이블은 AOMDV의 라우팅 테이블 엔트리를 확장하였다. 라우팅 테이블의 구조는 Destination, Sequence number, Advertised hop count, Route list, Expire time out 필드로 구성된다. 본 연구에서 고려한 내용은 이들 필드 중 Route list에 다중 경로를 선택하기 위해 Next Hop과 Hop count, Security level을 확장으로 보안경로와 최단일반경로를 선택할 수 있는 필드이다. 제안 프로토콜의 라우팅 테이블의 또 다른 특징은 Route list 필드의 라우팅 테이블의 Security Level 표기 기법이다. Security Level 표기법은 QoP(Quality of Protection) 비트 벡터를 적용으로, 네트워크에 존재하는 보안노드가 보안 레벨을 위해 4개의 다른 비트를 사용할 수 있다면, 이 4개의 비트로 보안 레벨 정보를 설정할 수 있도록 표현하는 것이 가능하므로 효과적인 정보표현을 할 수 있기 때문이다.

3.3 데이터 전송

제안 프로토콜로 보안경로와 다중일반경로를 발견한 출발지노드는 데이터 전송을 위한 단계를 처리한다. 출발지 노드는 가장먼저 보안 노드들과 공유된 마스터 키 를 이용해 데이터를 전송하기 위한 최단일반경로 정보와 데이터 전송경로를 강화하기 위한 세션 키를 인증정보와 함께 암호화하여 목적지 노드로 전달한다. 중간 보안노드들은 출발지 노드를 인증하고 다음 보안노드로 전달한다. 목적지 노드는 보안경로를 검증한 후 데이터 수신대기 정보를 보내, 최단일반경로로 출발지 노드에서 암호화된 데이터를 목적지 노드로 전달한다.

3.4 경로유지

Ad Hoc 네트워크에서는 악의적인 노드가 발견되거나 노드 이동으로 링크 손상과 같은 현상으로 인해 사용 중인 라우팅 경로의 손상을 초래할 수 있다. 특히 노드 이동성으로 인해 네트워크 링크가 손상되는 경향이 많다. 그림 5에서와 같이 노드 PN3이 손상되거나 악의적인 노드일 경우 손상된 링크에서의 링크 (PN2,PN3)의 전방 노드 PN3는 라우팅 테이블에서 링크 손상으로 도달할 수 없는 모든 수신 노드 정보를 무효화 시킨다. PN2는 손실된 수신 노드 정보를 포함한 RREQ를 생성하여 출발지 노드 S로 전송한다. 주목할 점은 RRER을 사용하는 경로 유지관리 측면에서 AOMDV 사이의 커다란 차이가 없다는 점이다.

Ⅳ. 시뮬레이션

4.1 시뮬레이션 환경

본 논문의 시뮬레이션은 현재 전 세계 적으로 이용되는 ns-2[11]을 이용한다. 실험에 사용한 ns-2의 버전은 ns-2.1b4a 버전을 사용하고 제안한 프로토콜의 구현을 위해 SAR은 ns-CMU 확장판에 포함된 AODV에 기반으로 구현하였다. 또한 AODV를 수정 보완된 AOMDV 기반으로 동작되는 시뮬레이션 플랫폼 상에서 MP-SAR 라우팅 프로토콜의 코어를 구현하여 적용하고 이를 비교분석 하였다.

본 시뮬레이션은 500 x 500 m2 의 정방향 영역상에서 움직이는 모바일 노드들을 대상으로 수행된다. 100m의 무선 전송 범위와 자유공간 전파채널을 가정한다. 2 Mbps의 데이터 전송률을 가지며, 각 시뮬레이션은 1000초 동안 수행된다. 출발지 노드

는 초당 5개의 패킷을 전송하며, 데이터 페이로드는 10000 바이트이다. 모바일 노드들은 불규칙하게 임의로 움직인다고 가정하며, 파라미터 중 최대 속도는 10 ~ 100 m/sec로, 일시정지 시간은 30sec로 설정한다. 본 시뮬레이션 연구에서 성능 척도를 측정하기 위하여 평균 노드 속도와, 보안노드의 수와 같은 시뮬레이션 인자를 의미 있는 범위에서 변화시킨다. 한 가지 시뮬레이션 인자를 변화시키는 동안에 나머지 인자들은 고정되는데, 평균 노드 속도는 20 m/sec, 일반노드의 수는 30, 보안노드는 20의 고정 값을 갖는다.

4.2 실험결과

본 절에서는 시뮬레이션 결과를 제시하고, 제안한 MP-SAR의 성능을 SAR과 비교 분석한다. 패킷 전달율, 라우팅 오버헤드 등 성능 척도를 평균 노드 속도, 보안노드의 수와 같은 시뮬레이션 인자 측면에서 광범위하게 평가 및 비교한다.

그림 5는 보안노드 수의 변화에 따른 SAR과 MP-SAR의 패킷 전송률의 변화를 나타낸다. 실험결과를 통해 알 수 있듯이 여러 보안노드를 경유하며 데이터 패킷을 보내는 것보다는 MP-SAR에서 제안한 바와 같이 최단경로를 이용해 데이터를 보냄으로써 더 좋은 성능을 보임을 알 수 있다. 특히 노

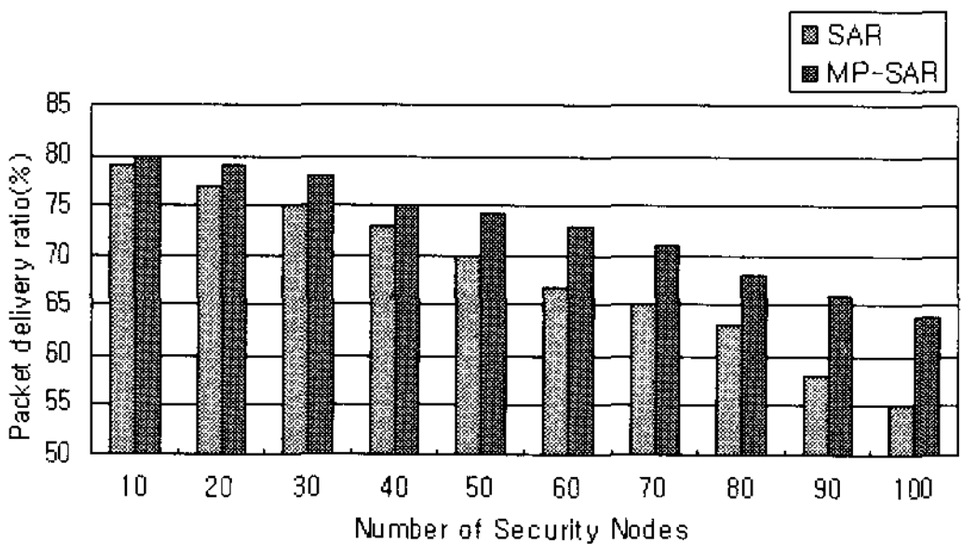


그림 5. 보안노드 수의 변화에 따른 패킷 전송률의 변화

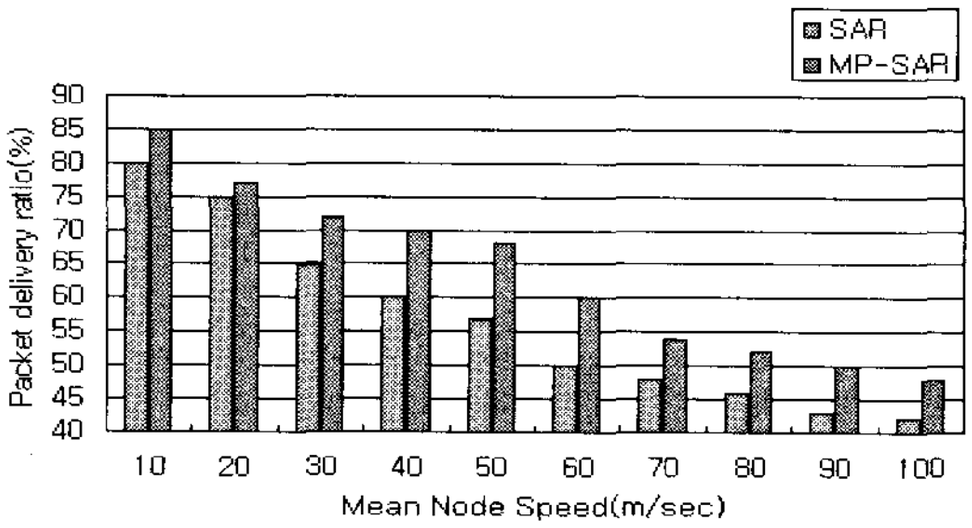


그림 6. 평균노드 속도에 따른 패킷 전송률의 변화

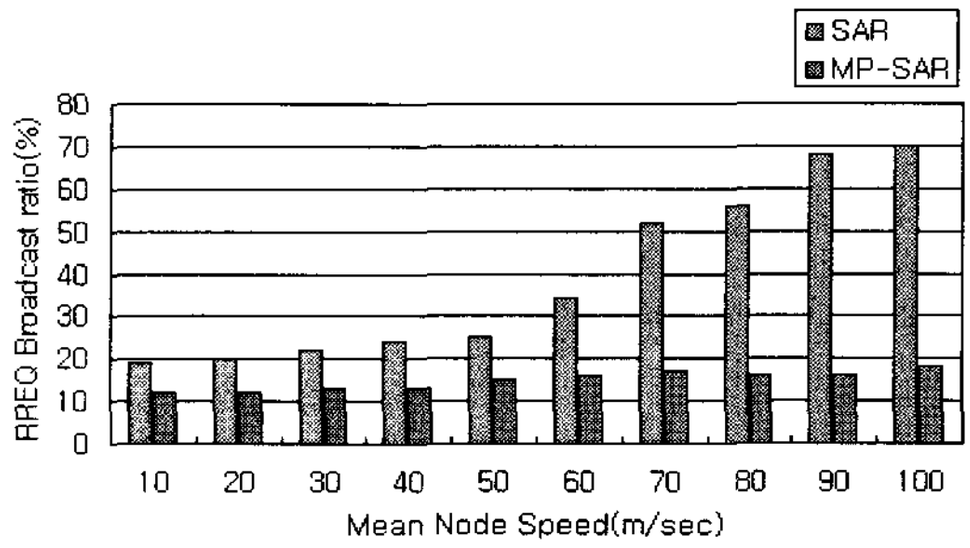


그림 7. 노드의 평균 이동속도에 따른 RREQ의 횟수율의 변화

드의 수가 증가함에 따라 그 차이가 더욱 커진다. 이는 노드 밀도가 높으면 출발지 노드와 목적지 노드사이에 더 많은 트래픽 간섭이 많이 발생하여 링크 손상 가능성이 증가한다.

그림 6는 노드의 평균 속도에 따른 SAR과 MP-SAR의 패킷 전달율을 나타낸다. 이는 높은 노드 이동성이 더욱 빈번한 링크 손상을 초래함으로써 많은 패킷이 버려질 수 있기 때문이다.

단일 경로를 보유한 SAR의 경우 노드의 이동으로 빈번한 경로 탐색이 발생하므로 노드의 이동속도에 따른 패킷 전달율이 급격히 감소하지만 MP-SAR의 경우 다중경로를 보유하므로 SAR보다는 패킷전달률에 있어 더 좋은 성능을 보인다.

그림 7는 노드의 평균 이동속도에 따른 RREQ의 횟수율을 나타낸다. 높은 노드 이동성은 더욱 빈번한 링크 손상을 초래함으로써 라우팅을 위한 보다 많은 RREQ패킷이 필요하게 된다. 다중경로를 보유한 MP-SAR은 RREQ의 횟수율에 있어서 큰 증가율을 보이지 않는 반면 단일경로를 갖는 SAR은 이동속도에 따라 RREQ의 전송 횟수율이 크게 증가함을 알 수 있다. 이상과 같은 실험결과에서 패킷 전달률과 라우팅 오버헤드 등의 성능 척도 모두에 대하여 MP-SAR이 보다 SAR보다 통신에 대한 성능이 우수함을 알 수 있다.

V. 결 론

SAR 프로토콜은 AODV 프로토콜을 기반의 프로토콜이기 때문에 데이터의 전송 중 중간노드가 전송을 중단하거나, 중간노드의 이동으로 데이터 전달 범위를 벗어날 경우 라우팅 경로를 처음부터 재탐색하게 되어 전송시간 지연 문제가 발생한다.

본 논문에서는 데이터의 인증을 위한 보안경로와 데이터를 전송하는 데이터 전송경로를 포함한 다중

경로기법을 제공하고 있어 기존의 SAR 프로토콜과 동일한 데이터의 신뢰성을 유지하며 데이터 전송 속도의 성능을 높이는 새로운 MP-SAR 프로토콜을 제안하였다. 또한 그 성능의 우수함을 실험결과를 통해 알 수 있었다. 향후 연구에서는 보안노드의 인증메커니즘을 최적화하여 보안경로 탐지의 지연을 최소화 하고자 한다.

참 고 문 헌

〔1〕 이병진, 유상조, "애드 혹 네트워크에서 소스 기반 다중 게이트웨이 선출 라우팅 프로토콜", *한국통신학회논문지 No.8A*, Vol.30, pp. 679-680, 2005.

〔2〕 J. Broch and D. B. Johnson, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," *IETF Internet Draft*, October 1999.

〔3〕 C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in The Second IEEE Workshop on Mobile Computing Systems

〔4〕 E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," *IEEE Personal Communications*, Apr. 1999.

〔5〕 S. Marti and T. Giuli and K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile ad hoc networks," *in The Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Boston, MA, USA, Aug. 2000.

〔6〕 Y. Ko and N. H. Vaidya, "Location-Aided Routing(LAR) in Mobile Ad Hoc Networks," *in The Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, USA, Oct. 1998.

〔7〕 V. D. Park and M. S. Corson. "A Highly Adaptive Distributed Routing Algorithm Wireless Networks," *In Proceedings of IEEE Infocom*, pp.1405 - 1413, 1997.

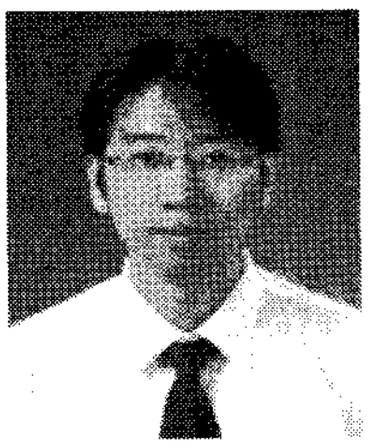
〔8〕 J. Raju and J. J. Garcia-Luna-Aceves,"A New Approach to On-demand Loop-Free Multipath Routing," *In Proceedings of the Int''l Conf. on Computer Communications and Networks (IC3N)*, pp.522 - 527, 1999.

〔9〕 Y. Seung and P. Naldurg and Robin Kravets, "Security-Awares Ad Hoc Routing for Wireless Networks," *In Proceedings of MobiHOC*, Oct,2001

〔10〕 L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, Nov. 1999.

〔11〕 K. Fall and K. Varadhan, The ns Manual, UC Berkeley, LBL, USC/ISI, Oct. 2001, Available at http://www.isi.edu/nsnam/ns

한 인 성 (In-sung Han) 정회원



2001년 2월 배재대학교 컴퓨터공학과 학사졸업
2004년 8월 광운대학교 컴퓨터과학과 석사졸업
2004년 9월~현재 광운대학교 컴퓨터과학과 박사과정

<관심분야> 애드 혹 네트워크 보안, 센서 네트워크 보안, 무선 서비스 발견 및 전달

유 황 빈 (Hwang-bin Ryou) 정회원

1975년 2월 인하대학교 전자공학과 공학사 졸업
1977년 2월 연세대학교 대학원 공학석사 졸업
1989년 2월 경희대학교 대학원 공학박사 졸업
1981년 3월~현재 광운대학교 컴퓨터소프트웨어학과 교수

<관심분야> 멀티미디어통신, 네트워크 보안, 무선네트워크 보안, 센서 네트워크 보안