한국마린엔지니어링학회지 제33권 제1호, pp. 120~130, 2009. 1 (ISSN 1226-9549)
Journal of the Korean Society of Marine Engineering

이동 다중 홉 무선망 모델에 기반한 해양통신망을 위한 경로배정 보안 연구

문성미* · 손주영†

(원고접수일 : 2008년 7월 30일, 원고수정일 : 2008년 9월 16일, 심사완료일 : 2008년 9월 22일)

A Study on Secure Routing for a Maritime Network Based on Mobile Multi-hop Wireless Networks

Seong-Mi Mun* · Joo-Young Son†

Abstract : In recent years, many mobile wireless communication devices and applications have been deployed on the planet. The mobile multi-hop wireless network models appeared to provide means to access to networks where few infrastructure exists. However, the mobile multi-hop wireless networks have weaker points in attacks and intrusions than the wired and one-hop wireless networks. In this paper, the secure routing issues in most mobile multi-hop wireless network models are surveyed in depth. The state-of-the-art technologies and research activities are explained. Finally, the issues and technologies for the secure routing specific to a maritime network model are sufficiently discussed as conclusions.

Key words : Mobile Ad-hoc networks(모바일 애드 혹 네트워크), Mobile multi-hop wireless networks(이동 다중 홉 무선망), Security(보안), Routing protocol(경로배정 프로토콜), Maritime networks(해양통신망)

1. 이동 다중 홉 무선망 소개

최근 무선기기와 무선 네트워크의 사용이 급격히 확산되고 있다. 이동 다중 홉 무선망은 MANET (Mobile Ad hoc Network), WSN(Wireless Sensor Network), WMN(Wireless Mesh Network), VANET(Vehicular Ad hoc Network) 등의 형태로 매우 다양하고 유선망을 형성하기 어려운 전쟁터, 재난 지역 등 유선 설치가 힘들거나 비용이 많이 드는 응용에 적용하고자 하는 노력이 계속 되고 있다. 이러한 이동 다중 홉 무선망은 이동 노드가 망을 형성하기 위해 서로 협력하고 노드가 제한된 전력, 계산 능력 등을 갖는 것이 일반적이다. 하지만 여러 다양한 이동 다중 홉 무선망의 기본 형태인 MANET과는 근본적인 차이가 존재하는데 WSN의 경우 망 자체가 하나의 응용이고 센서 노드가 매우 저가인데 이에 따라 계산 능력, 저장 공간, 통신 능력이 상당히 제한적이다[1]. WMN에서 노드는 유선망과 별반 다르지 않으며 무선으로 동작하는 라우터를 여러 번 거쳐 유

† 교신저자(한국해양대학교 컴퓨터제어전자통신공학부, E-mail:mmlab@hhu.ac.kr, Tel: 051)410-4575)
* 한국해양대학교 컴퓨터공학과 네트워크 연구실

선 인터넷을 통해 데이터를 전송한다[2]. VANET을 구성하는 노드는 도로 상의 차량으로 이동이 매우 빠르고 잦은 노드 밀도와 망 위상 변화 등의 특징을 가진다[3].

각 이동 다중 홉 무선망은 형성이나 활용에 여러 가지 유연성을 제공하나 망의 크기가 커짐의 따라 그 특성으로 인해 공격과 침입에 대한 취약점이 드러나고 있다[4]. 2장에서는 이동 다중 홉 무선망이 갖는 보안 취약점을 살펴보고 3장에서 각 이동 다중 홉 무선망의 보안기법과 최근 연구 동향을 살펴본다. 4장에서는 해양통신망 모델을 소개하고 그에 따른 보안 기법을 제시하고 5장에서 결론을 맺는다.

2. 이동 다중 홉 무선망의 보안 취약점

이동 다중 홉 무선망은 유선 통신망과는 다르게 무선 링크를 사용하므로 도청, 통신 비밀성, 익명성을 위협하는 수동적인 공격과 공격자가 망에 패킷을 보내 노드와 타협하고 노드의 정보를 유출시키거나 통신을 방해하는 등 능동적인 공격에 모두 취약하다. 물리적인 방화벽이나 게이트웨이 등의 일차적 방어가 불가능하기 때문에 모든 노드가 공격 대상이 된다. 이동 다중 홉 무선망은 공통적으로 망을 자율적으로 형성하기 때문에 모든 노드가 망에 접근하는 것이 가능하나 노드의 신뢰성을 보장하기가 어렵다는 특징을 갖는다. MANET의 경우 노드는 가끔 이동하기 때문에 망의 위상이 지속적으로 변화하고 노드의 제한된 전력을 절약하기 위해 통신을 일시적으로 중단하기도 한다. 만약 망의 위상이 급격하게 변화하는 경우 망 내에서 정상적인 노드가 악의적인 노드를 구별하기는 어렵다. WSN의 경우 응용의 특성 때문에 노드가 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 쉽게 변경되기도 하고 역시 악의적인 노드가 망에 연결되어 불필요한 정보를 발생시킬 수 있다[5]. WMN 역시 MR(Mesh Router)의 물리적 위치 때문에 외부 공격에 쉽게 노출되고 공격자의 조작에 의해 악의적인 기능을 수행할 가능성이 높다. VANET의 대표적인 응용은 차량 간 충돌 경고, 교통상황정보 등을 보장하는 것인데 공격자가 이를 악용하면 교통상황을 혼란하게 하여 큰 위험을 초래할 수 있다. 또한 노드의 특성상 잦고 큰 이동성 때문에 잦은 핸드오버가 발생한다. 이때 이전 주소와 새로운 주소를 신속하게 바꿔주어야 하는데 그렇지 못할 경우 이 과정을 악의적으로 사용하여 여러 공격을 수행할 수 있다.

이러한 이동 다중 홉 무선망은 첫째, 노드의 제한된 통신, 계산 능력과 작은 메모리 등의 특성을 가지므로 기존 유선망에서의 보안 기술을 적용하기에 적합하지 않고 둘째, 멀티 홉 기반의 무선 통신을 하기 때문에 트래픽이 도청당하거나 방해 전파에 의해 훼손될 가능성이 크고 셋째, 노드 간의 상호 작용으로 자율적으로 망을 형성하기 때문에 효과적인 관리나 보안 기능 강화가 어렵다는 공통점을 가진다.

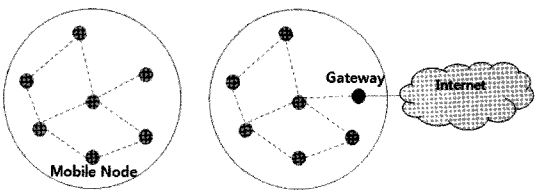
3. 이동 다중 홉 무선망에 대한 보안

노드는 서로를 신뢰하지 않고 망의 위상은 지속적으로 변화하기 때문에 개별적으로 공격에 대응하는 노드나 기능을 한 곳에 집중시키거나 별도로 통신을 위한 인증 등의 과정을 거치기는 어렵다. 노드의 이동성과 노드의 자원 부족 등을 고려하면 망에 대한 공격이나 이에 대한 적절한 방지는 복잡하지 않고 빠른 처리가 가능해야 한다. 따라서 경로배정 과정과 동시에 노드나 망의 안전성을 인증하는 것이 효율적이다.

무선 경로배정 프로토콜에 대한 공격은 일반적으로 경로배정 붕괴 공격과 자원 소비 공격으로 나뉜다. 경로배정 붕괴 공격은 공격자가 역기능적 방법으로 경로를 설정하는 패킷을 만들어내려는 시도이다. 자원 소비 공격은 공격자가 패킷을 망으로 계속해서 발생시키는 것으로 대역폭이나 노드의 메모리, 전력을 낭비시키고자 하는 것이다. 에너지와 가용한 대역폭을 고갈시키기 위해 경로배정 루프를 유발하는 경로배정 패킷을 발생시키는 것이다[6]. 이동 다중 홉 무선망에서는 이러한 공격 유형뿐 만 아니라 앞서 설명한 망의 특성으로 인한 취약점을 보호할 수 있어야 한다.

3.1 MANET에서의 보안

MANET은 상이한 전송 능력과 이동성을 가지는 노드들이 망에 동적이고 임의적으로 접속하고 그 구성은 시간에 따라 임의로 바뀌는 특성을 가진다. 고정 기반망이나 AP(Access Point), BS(Base Station)와 같은 중앙 관리 없이 동작하는 이동 노드가 자율적으로 망을 형성하기 때문에 노드는 종단 노드와 중간 노드의 역할을 동시에 해야 한다. MANET의 이러한 특징은 이동 노드들이 활용할 수 있는 자원 즉, 대역폭, 노드의 전원, 노드의 계산 능력 등을 더욱 부족하게 한다. 또한 통신은 이동 노드 간 안테나를 이용하여 무선 링크를 통해 이루어지는데 노드들은 상이한 전송 능력을 가지기 때문에 높은 전송 전력을 가진 노드와 낮은 전송 전력을 가진 노드 간에 단방향 링크가 형성된다[7]. 전력 제한, 채널 효율성 등을 고려하여 이동 노드는 단일 홉 방식으로 다른 노드와 직접적으로 통신을 할 수 없고 여러 중간 노드를 거쳐 원하는 목적 노드와 통신을 한다. MANET은 고정 기반망 등을 이용하기가 어렵거나 비용이 많이 드는 경우 즉, 군사 지역, 재난 지역, 외부 업무 시 등에 활용된다[8]. MANET은 Fig. 1 (a)와 같이 이동 노드들 간 통신을 통해 망을 형성하는 일반적인 형태와 (b)와 같이 하나의 노드가 게이트웨이 역할을 하여 인터넷과 연동하도록 확장한 형태가 있다.



(a) Independent (b) Connected with wired network

Fig. 1 Architecture of mobile ad hoc networks

MANET에서는 멀티 홉 방식으로 경로배정이 수행될 경우 악의적인 중간 노드로부터 데이터의 무결성 및 기밀성에 문제가 발생할 수 있다. SAR(Security Aware Routing)은 AODV(Ad Hoc On-demand Distance Vector) 기반의 보안 경로배정 프로토콜로 서로 다른 Ad hoc 노드의 보안 속성을 이용해 안전한 보안경로를 설정한다. 경로배정에 이용되는 메트릭을 노드의 보안 레벨로 이용하여 노드 간 신뢰 관계를 형성하도록 한다. 노드가 경로 설정을 할 때 전송 경로 상의 노드들의 보안 레벨을 체크하고 레벨이 낮으면 레벨이 높은 노드를 거치는 다른 경로를 선택하는 방식이다[9]. 기존의 경로배정 프로토콜을 그대로 이용하여 간단한 접근 방식이나 보안 레벨이 높은 노드만을 통해 데이터를 전송하기 때문에 선택된 경로는 최적의 경로가 아닐 가능성도 있다. 최근 연구 가운데 SAR의 문제점을 개선하기 위한 것이 있다. SAR의 보안 기법을 확장한 MP(Multi Path)-SAR은 다중경로를 탐색하고, 이 중 유효한 최단경로를 이용해 빠르고 신뢰성 있는 데이터 전달을 하는 방법이다[10]. 이는 SAR이 단일 노드의 보안 레벨만을 점검하는 것과 달리 유효한 여러 경로를 찾고 그 중 가장 안정한 전송경로를 설정하므로 경로 설정 부하나 경로의 최적성 면에서는 좋다. 그러나 노드들이 모두 UID(Unique Identifier)를 가지고, 임의의 노드 A, B는 양방향 통신이 가능해야 하고, 모든 노드에 보안 레벨 속성이 정의되어 있어야 하는 등의 많은 가정 사항을 가진다.

3.2 WSN에서의 보안

WSN은 센서 노드로 형성된 망으로 특정 환경에 대한 정보를 수집하는 것을 특징으로 한다. 데이터를 수집하고자 하는 지역에 수백, 수천 개의 센서 노드를 설치하여 구성한다. 센서 노드는 온도, 압력, 소리의 세기 등을 센싱하여 가공할 수 있는 프로세서가 장착되어 있고 이를 전송할 수 있는 송수신기를 갖는다. 싱크 노드는 WSN 내의 센서 노드들을 관리하고 제어하며 센서 노드들이 센싱한 정보를 수집하고 인터넷 등 외부 망으로 연결하는 게이트웨이 역할을 수행한다. Fig. 2는 앞서 설명한 WSN의 가장 일반적인 형태이다. WSN은 군사 목적, 공장 자동화, 날씨/기후 예측 등을 위해 활용된다[11].

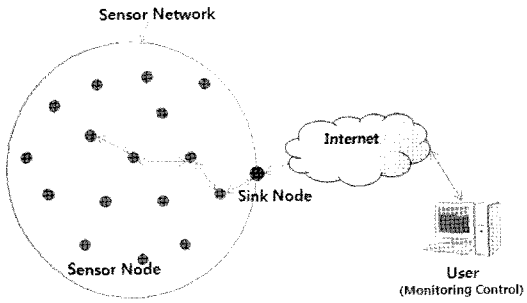


Fig. 2 Architecture of a wireless sensor network

센서 노드의 가격은 매우 저렴하고 이에 따라 계산 능력, 저장 공간, 통신 능력 등이 제약되어 있다. 이처럼 자원이 매우 제약되어 있기 때문에 기존의 MANET 경로배정 기법이 적용되기 힘들고 이러한 특성을 고려한 보안이 필요하다. SEEM (Secure and Energy-Efficient Multipath routing protocol)은 멀티패스 기법으로 대부분의 작업을 BS에서 처리하도록 한다[12]. 망을 구성하기 위해 BS는 neighbors discovery 메시지를 보내고 메시지를 받은 각 노드는 메시지에 저장된 주소를 테이블에 저장하고 메시지의 주소를 자신의 주소로 바꾸어 다시 이웃 노드에 전송한다. 이를 반복하여 각 노드가 이웃 노드의 테이블을 저장하면 BS는 이 테이블을 취합하고 전체 망의 정보를 알 수 있다. 데이터의 전송은 BS의 요청에 따라 이루어진다. BS가 요청 메시지를 전체 망에 전송하면 해당 데이터를 지닌 노드는 응답 메시지를 BS로 전송하는데 이 메시지는 전달 경로의 각 노드의 첫 번째 테이블 첫 번째 노드를 통해 전달한다. 전달되는 경로는 BS가 결정하고 경로를 선택할 때 각 노드의 남은 에너지 수준을 고려하여 에너지의 균형을 맞추기 때문에 망의 트래픽을 전체 노드에 고르게 분산시킨다. 효율성이 높으나 포획 노드를 탐지할 수는 없다. 보안 대안 경로 경로배정(secure alternate path routing)은 다중 경로(Multipath) 기법으로 각 노드는 여러 개의 BS까지의 경로를 저장하여 라운드 로빈 형태로 각 메시지를 다른 경로로 전송한다[13]. 이웃 보고 시스템(Neighbor report system)을 이용하여 경로배정 업데이트 메시지를 구성한다. 메시지를 받은 노드는 단방향 해시 함수를 이용해 메시지를 검증하여 포획된 노드를 판단해 낸다. 포획된 노드를 탐지하는데 적극적인 형태이므로 안정성이 높으나 상대적으로 계산량이 많다.

3.3 WMN에서의 보안

WMN은 전통적인 MANET과는 달리 고정 노드와도 연결하여 망을 형성하고 그렇게 형성된 망이 인터넷과 연동된다. 현재 이동 다중 홉 무선망 분야에서 최대의 이슈는 WMN이다. 사용자들에게 last mile 광대역 인터넷 서비스를 제공하기 위해서 가장 효율적인 솔루션 중의 하나이다. WMN은 MR과 MC(Mesh Client)로 구성되는데 MC는 WMN에 연결되는 단말이고, MR은 사용자에게 무선랜의 AP처럼 서비스를 제공하고 고정 노드와 연결되며 인터넷과 연동된다. MR은 자가 구성(Self-configuration), 자가 치유(Self-healing) 등의 기능을 갖추어야 하고 멀티 홉 경로배정을 통해 유선 인터넷 노드까지 패킷을 전달해 주어야 하기 때문에 기존의 AP보다 다양한 기능을 할 수 있어야 한다. MR은 다른 MR하고만 통신하는 것이 있고, 또 다른 MR 뿐 아니라 일반 컴퓨터와 통신하는 것이 있는데 후자의 경우는 MAP(Mesh Access Point)라고 한다[14]. Fig. 3은 WMN의 가장 일반적인 형태로 MR과 MC가 게이트웨이를 통해 인터넷과 연동되는 형태를 보여준다.

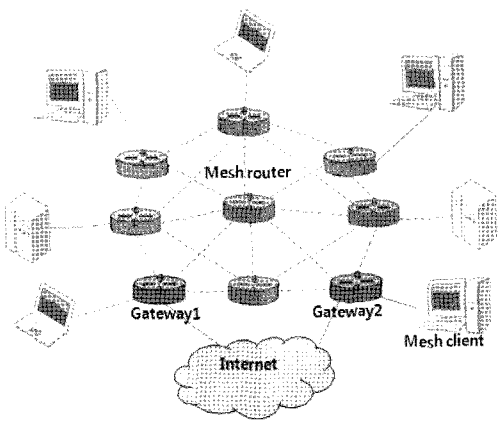


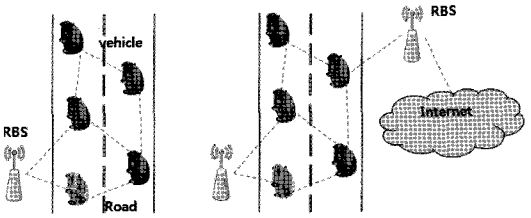
Fig. 3 Architecture of a wireless mesh network

WMN은 last mile 광대역 인터넷 연결, MAN (Metropolitan Area Network), 기업망, 교통망, 빌딩 자동화, 의료 시스템 등에서 유용하게 활용된다.

WMN는 라우터가 대부분 외부의 고정된 장소에 위치하기 때문에 공격자가 쉽게 접근하여 경로배정 정보를 공격할 수 있고, 경로배정 과정에 참여하면서 테이블을 의도적으로 갱신하지 않는 등의 공격을 할 수 있다. 따라서 WMN에서는 노드 간 신뢰 관계를 구축하는 것이 중요하다[15]. ARAN (Authenticated Routing for Ad hoc Networks)은 인증서를 이용한 경로배정 기법이다. ARAN에서 소스 노드는 경로 발견 메시지를 브로드캐스트하며 각 경로 발견 메시지는 소스 노드에서 목적 노드로 이르는 각 홉에서 인증된다[16]. 경로 상의 노드가 모두 인증서를 추가하고 검토 하는 등 중간 노드에 대한 인증을 하고 있으나, 경로 요청과 응답 과정에서 모든 노드들은 경로배정 관련 작업을 수행하고 패킷을 전송할 때마다 자신의 인증서를 부가적으로 추가하여 전송해야 하는 단점이 있다. SRP(Secure Routing Protocol)는 임의의 두 단말 상에 공유된 비밀키를 가정한다. 패킷의 신선함(Freshness)을 보장하기 위해 순서 번호를 사용하여 경로배정 루프나 여러 악의적인 패킷의 영향을 피할 수 있으나 문제는 목적 노드 간에 존재하는 중간 노드에 대한 인증 과정이 없다는 것이다[17]. 최근 연구 가운데 WMN의 보안 이슈 가운데 인증과 무선 경로배정 프로토콜을 함께 이용하는 방법이 있다[18]. 경로배정 과정에 기초하여 중앙 관리자 역할의 노드 없이도 빠르고 안전하게 인증을 하고, 중간 노드에 의한 공격을 방지하기 위해 중간 노드에 대한 인증도 수행하도록 하는 방법이다. 그러나 이 논문에서는 WMN를 2 홉 정도의 홈 네트워크로 한정짓고 있어 2 홉 이상의 WMN에서는 어떠한 성능을 보이는지에 대해서는 고려하지 않고 있다.

3.4 VANET에서의 보안

VANET은 노드가 도로를 따라 정해진 이동 경로에 있는 차량 내 통신 장치 간 통신을 가능하게 한다. 각 노드는 GPS(Global Positioning System)를 통해 다른 노드의 위치를 획득하는 것이 가능하고 망의 위상이 아주 빠르고 빈번하게 변한다. 또한 멀티 홉 경로배정은 차량의 밀도에 의존하는데 차량의 이동 속도 및 방향이 도로에 따라 정해진 이동 경로를 가진다는 특성이 있다. 차량 간 충돌 경고, 노변신호 알림, 교통상황정보 등 운전 시 중요한 정보를 제공하는 것부터 각종 멀티미디어 전송, 인터넷 서비스 그리고 톨게이트 및 주차장 자동요금징수 등 차량 탑승자에게 안전 및 편리함을 제공하는 응용 서비스를 제공한다[19]. Fig. 4 (a)는 V2V(Vehicular-to-Vehicular) 환경으로 차량과 차량 사이 또는 차량과 RBS(Roadside Base Station) 사이에서 교통안전 정보를 제공해주고, (b)는 V2I (Vehicular-to-Infrastructure) 환경으로 차량 내 단말 또는 사용자 휴대용 단말 등을 사용하여 인터넷 서비스를 이용할 수 있는 구조이다.



(a) V2V (b) V2I

Fig. 4 Architecture of vehicular ad hoc networks

VANET의 대표적인 응용은 차량 간 충돌 경고, 노변신호 알림, 교통상황정보 등 교통 환경의 안정과 효율성을 보장하는 것인데 안전한 통신이 이루어지지 않으면 이러한 큰 장점은 반대로 큰 재앙이 된다. 공격자가 왜곡된 정보나 정상적인 메시지 송신을 방해하면 심각한 위험을 초래한다. 또한 위치 기반이고 이동성이 크기 때문에 위치 익명성과 잦은 핸드오버를 안전하게 보장하는 것이 중요하다. PBR(Position Based Routing)은 기본적으로 넓은 지역에 걸쳐 확장성있고 효과적인 전달(Forwarding)과 변덕스러운(Volatile) 애드 혹 망을 제공한다. 비커닝(Beaconing), 위치 서비스

(Location service), 전달의 세 가지 서비스를 지원한다. 최근 여기에 암호 보호(Cryptographic protection), 가능성 점검(Plausibility checks), 강건성 매커니즘(Robustness mechanism)을 더하여 보안성을 추가한 연구가 있다[20]. 암호보호는 비대칭 암호화와 전자 서명을 이용하여 홉 간 그리고 종단 간의 인증과 무결성을 제공하는 것이고, 가능성 점검은 패킷 수신 시 순서대로 다른 점검을 실행하고 그것이 실패하면 패킷을 버리는 것이다. 강건성 매커니즘은 잘못된 다중 홉 플러딩 등으로 인해 망의 자원을 낭비하는 것을 막기 위해 어떤 노드가 특정 비율 이상으로 많은 패킷을 만들어내면 해당 패킷을 전달하지 않는 것이다. 또 다른 연구로 빠른 이동성을 지원하여 VANET에서 핸드오버 시 일어나는 공격을 방지하고자 하는 Fast MIPv6 핸드오버 인증 프로토콜을 제안한 것이 있다[21]. 이동 노드와 이전 라우터 간에 형성되어 있는 SA(Security Association)를 기반으로 모바일 노드와 다음 라우터 사이에서 DH(Diffie-Hellman) 알고리즘을 이용하여 핸드오버 인증키를 교환한다. 제안한 프로토콜은 단말에서 DH 지수 연산에 따른 오버헤드를 줄이기 위해 단말의 DH 공개키 지수 연산을 라우터에게 위임하는 Light-weight DH 방식을 사용한다. 기존의 핸드오버 인증 프로토콜은 한정적인 이동을 고려하여 설계된 것이나 이는 light-weight DH 알고리즘을 사용하여 안전하고 이동 단말에서 수행하는 연산량을 줄인 것이 특징이다.

3.5 IEEE 802.11 ad hoc mode에서의 보안

IEEE 802.11은 LAN에서 차량 속도나 보행 속도로 움직이는 이동성을 가지거나, 고정, 휴대용 노드의 무선 접속을 위해 MAC과 PHY 기능을 제공하는 표준이다[22]. 802.11은 IBSS (Independent Basic Service Set) 망과 ESS(Extended Service Set) 망을 지원한다. BSS(Basic Service Set)는 802.11 구조의 기본적인 구성 단위로 단일 조정 기능(Single coordination function)의 직접적인 제어 아래에 있는 노드들의 집합이다. Ad Hoc 망은 기반망의 도움 없이 상호 망 통신의 목적을 위해 단일 BSS로 노드들을 묶어 놓은 것이다.

최근 이러한 IEEE 802.11 기반의 무선랜 시스템은 단말에 대한 원활한 이동성 지원, 확장성 있는 망 구축 등 유선 망에 뒤지지 않는 고속의 전송 속도를 지원하여 초고속 무선망의 기반 구조로 입지를 다지고 있다. 그러나 보안 문제와 이동성 지원 문제로 무선랜 확대를 지연시키고 있다. 공중매체를 통해 브로드캐스트되기 때문에 도청 등의 공격에 노출될 수 있고 취약한 보안인증으로 인해 망에 쉽게 접근할 수 있다. 게다가 단말의 이동과 핸드오프에서 발생하는 지연은 실시간 멀티미디어 서비스를 지원하지 못한다[23]. IEEE 802.11i 태스크그룹은 국제 무선랜 보안표준을 제정하였다. 접근제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 그리고 무선구간 데이터 보호를 위한 새로운 대칭키 암호 알고리즘의 적용 등의 내용이다. 이를 통해 상위 사용자 레벨의 보안 인증 및 사용자 데이터에 대한 안전성을 제공해준다[24]. 하지만 단말의 핸드오프 시 마다 IEEE 802.11i 의 보안 절차에 따라 사용자 인증 절차를 수행해야 하므로 이때 발생하는 지연시간은 끊김없는 멀티미디어 서비스를 제공하지 못한다. 최근 연구 가운데 기본적 보안을 제공하면서, 핸드오프 시 단말의 사용자 인증 처리로 인한 지연시간을 줄일 수 있는 고속 사용자 인증 방법을 제시한 것이 있다[25]. 단말에 정상적인 사용자인증을 지원하는 AP(Access Point)로의 핸드오프를 위한 정보 제공, 단말의 실질적인 핸드오프가 가능한 선택전인 AP들에 대한 사전 인증, 마지막으로 단말의 모빌리티 상황에 따른 효율적인 단말의 인증정보 관리 기능을 제공한다.

3.6 MMR WiMax(WiBro)에서의 보안

광대역 무선 MAN의 전개와 개발을 지원하기 위한 광대역 무선 액세스 표준이다[26]. 도심 및 부도심지에서의 고정수신 안테나와 가입자 장치를 이용하여 10~66GHz 대역의 가시(Line-of-Sight) 통신환경에서의 서비스를 제공하기 위한 PHY 및 MAC 규격이다[27]. WiBro는 정지 또는 이동 중인 가입자에게 약 3Mbps 정도의 초고속 무선 인터넷

서비스와 60km/h 정도의 중저속 이동성을 보장할 수 있고, WiMax는 약 50km의 커버리지와 70Mbps의 전송속도를 제공할 수 있으며, 음성과 데이터 및 영상서비스를 모두 지원할 수 있다[28].

Mobile WiMax(WiBro)의 보안 구조는 기본적으로 일반적인 IEEE 802.11과 같은 무선망의 보안 기능을 근간으로 한다. 여러 기술 중 보안 관점에서 IEEE 802.16 표준은 MAC계층 안에 PKM (Privacy Key Management)이라는 보안 부계층(Security Sublayer)을 가진다. 이것은 기본적인 인증 및 기밀성 기능을 제공한다. 이후 IEEE 802.16 표준에서 향상된 보안 기능을 제공하는 PKMv2를 제공하며 기존 표준안의 부족한 점을 보완하기 위해 EAP(Extensible Authentication Protocol) 인증, AES(Advanced Encryption Standard) 기반 기밀성 알고리즘, CMAC/ HMAC (Cipher/Hashed Message Authentication Code)을 사용한 메시지 인증 기능 제공 등 보다 다양한 보안 기능을 제공하였다[29].

IEEE 802.16j에서는 MMR(Mobile Multi-hop Relay)을 도입하여 영역 확장 등의 목적으로 MMR-BS(Mobile Multi-hop Base Station) 등을 정의하고 있다[30]. 이러한 이동 멀티 홉 무선망에서는 망 구성을 쉽게 하기 위해 이동 멀티 홉 노드들이 무선으로 설치되고, 자가 구성과 자가 치유의 특성을 가지기 때문에 관리가 용이하다. MMR에서는 중앙 집중 보안 제어를 통해 보안을 제공한다. MS(Mobile Station)와 MMR-BS 사이에서 SA를 갖고 RS(Relay Station)에서는 어떠한 인증도 하지 않는다. MAC 관리 메시지와 비슷하게 모든 PKM 메시지는 MS와 MMR-BS사이에서 교환된다. PKM 메시지는 MS로부터 메시지 인증 코드에 의해 보호받지 못하기 때문에 다음 설명하는 과정을 거친다[31]. 이 경우에도 접근(access) RS와 중간(intermediate) RS는 단순히 PKM 메시지를 전송하는 역할을 한다. MS에서 인증되지 않은 PKM 메시지를 수신하면 접근 RS는 메시지에서 MMR-BS와 자신 사이에 만들어진 SA를 바탕으로 HMAC/CMAC을 추가한다. HMAC/CMAC을 추가한 PKM 메시지를 수신하면 MMR-BS는 접근 RS와 자신 사이에 공유된 SA를 기반으로 메시지를 인증한다. MMR-BS가 PKM 메시지를 MS로 발생시키면 자신과 접근 RS사이에 만들어진 SA를 기반으로 HMAC/CMAC을 추가한다. 이 메시지를 수신한 접근 RS는 자신과 MMR-BS사이에 만들어진 SA를 기반으로 하여 메시지를 인증한다. 메시지가 유효하면 HMAC/CMAC을 제거하고 MS로 PKM 메시지를 송신한다.

4. 해양통신망을 위한 보안

4.1 해양통신망 모델

해양통신망은 MANET의 기본적인 특징과 VANET의 특징을 갖고 있다. 해양통신망은 MANET과 같이 노드는 선박 내 통신 장치가 되고 중앙 통제 없이 노드 간 링크를 형성하여 통신망을 형성할 수 있다. 경제적인 이유로 최단 거리인 항로를 따라 이동하기 때문에 VANET처럼 이동 경로가 정해져 있다. 하지만 MANET의 노드 특성과는 다르게 육상의 고정 노드와 같이 자원이 풍부하고 VANET과는 다르게 이동 속도가 크게 빠르지 않기 때문에 위상 변화가 빈번하게 일어나지 않는다.

이러한 특성을 이용하여 새로운 해양통신망을 제안하였는데, 제안하는 해양통신망 모델(graph, G)은 정적 정보와 동적 정보로 정의하여 구성하고 각각 그래프 G_1과 G_2로 표현한다[32]. 항로의 출발 및 종착점인 항구(harbor, h),항로와 항로의 교차점(cross point, cp)들의 집합을 V_1이라 하고, 이들을 잇는 항로의 일부분으로서의 항구와 항구, 항구와 교차점, 교차점과 교차점을 잇는 선분들의 집합을 E_1로 정의한다. Fig. 5를 예로 살펴보면 $V_1=(h_1, h_2, h_3, h_4, cp_1, cp_2 \cdots cp_{11})$이 되고, $E_1=(\{h_1, h_2\}, \{h_2, h_3\} \cdots \{h_1, cp_1\}, \{h_1, cp_2\} \cdots \{cp_1, cp_2\} \cdots)$이 된다. 이를 정적 정보라고 하고 $G_1=(V_1, E_1)$로 표현한다. cp 영역은 선박이 가지는 전송시스템의 전송범위 내에 2개 이상의 항로를 포함하는 영역을 말한다. 상호 통신하고자 하는 항로 상의 임의의 선박들(s, d)을 V_2로 정의한다. Fig. 5를 보면 E_1 가운데 s, d에 의해 분할되는

선분(e_1, e_2)이 생긴다. e_1이 s에 의해 양분되는 es_1, es_2와 e_2가 d에 의해 양분되는 ed_1, ed_2가 생기는데 새롭게 생긴 선분의 집합을 E_2라 하고, 이를 동적 정보 $G_2=(V_2, E_2)$로 한다. 따라서 모델(G)은 $G(V, E) = G_1(V_1, E_1 - \{e_1, e_2\}) \cup G_2(V_2, E_2)$이다.

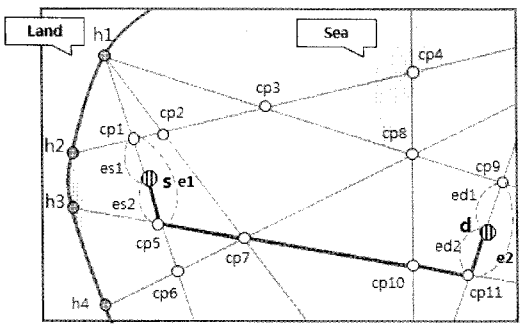


Fig. 5 Architecture of a maritime network

4.2 해양통신망에서의 보안

해양통신망에서는 항해 선박의 해상 안전, 재난 구조, 갑작스런 기상 변화 등을 주변의 선박에게 안전하고 신뢰성 있게 전달해주는 응용이 필요하다. 더 나아가서는 선박 간의 통신을 통해 일반적인 인터넷 서비스를 비롯하여 멀티미디어 서비스가 가능해야 한다. 해양통신망에서 선박 간 통신 시 멀티 홉 방식으로 경로배정이 수행되기 때문에 악의적인 중간 노드로 인한 데이터 무결성, 기밀성에 위협을 받을 수 있다. 또한 해적 등에 의한 공격이 있을 수 있으므로 위치 및 경로 익명성을 보장하여 각 선박의 비밀성을 유지해 주어야 한다.

제안하는 해양통신망에서의 경로배정은 앞서 설명한 정적 정보를 이용해 데이터 전송 요구가 있기 전에 모든 노드에 대한 경로를 파악하는 선행(Proactive) 경로배정과 동적 정보를 이용해 데이터 전송이 발생할 때에 목적지에 대한 경로를 파악하는 반응(Reactive) 경로배정을 결합한 혼합(Hybrid) 경로배정 방법을 이용한다[33]. 정적 정보를 이용하여 최단경로를 미리 계산하고 해당 정보는 모든 노드가 알고 있다. 출발지 노드가 데이터 전송을 원할 때 동적 정보를 이용하여 부분적으로 경로를 계산하여 최단경로를 선택한다. 이를 바탕으로 해양통신망에서 요구되는 경로배정 기법을 위한 보안 기술을 제시한다.

첫째, 안전한 경로배정을 위해 노드 간 신뢰성을 구축해야 한다. 해양통신망은 중앙관리 체제가 없기 때문에 각 노드 단위로 분산 인증을 수행해야 한다. 각 선박은 출항 전 인증을 위한 인증 상수와 호스트 키를 부여받고 경로 상의 노드인 선박을 인증하는 과정을 거쳐야 한다. 이러한 인증 방법은 [18]의 연구를 참고하여 인증 상수와 호스트 키, 시스템 시간, MAC(Media Access Control) 주소를 호스트 인증키를 이용하여 암호화한다. 경로 상의 중간 노드들에서는 출항 전 부여받은 호스트 키를 이용하여 메시지를 전달받은 노드의 호스트 인증키를 다시 생성하고 이를 이용해 메시지를 복호화하여 인증 상수를 구한다. 해당 중간 노드가 출항 전 부여받은 인증 상수와 비교하여 동일한 값이 있는지 찾아보고 있을 경우 적합한 노드라고 판단하여 다른 노드로 메시지를 전달한다. 시스템 시간은 릴레이 공격을 방지하고, MAC 주소 또한 메시지를 전달하는 노드의 MAC 주소와 메시지 내의 MAC 주소를 대조하여 동일하지 않을 경우 공격으로 간주할 수 있다. 이러한 방법을 통해 출발지 노드와 중간 노드들, 목적지 노드 모두 인증할 수 있다. 해양통신망의 경로는 이미 알고 있으므로 신속하게 경로를 찾을 수 있고 해당 경로 상의 노드에 대해서만 수행하면 된다. 다른 이동 다중 홉 무선망에서 경로 발견 과정에서 브로드캐스팅을 하면서 인증을 수행하는데 반해 해양통신망에서는 일정 노드에 대해서만 인증을 수행하면 되므로 신속한 처리가 가능하다.

둘째, 암호화 등을 통해 데이터 자체의 기밀성, 무결성 보장이 필요하다. 무선 구간으로 전송되는 모든 데이터를 암호화하여 전송하고 암호 알고리즘에 사용되는 키 또한 출항 전 부여받아 적용할 수 있도록 한다[34]. 일반적으로 암호에 사용되는 키는 중앙 서버를 통해 주기적으로 갱신되는 것이 보통이나 해양통신망에서는 중앙 서버의 역할을 할 수 있는 노드가 없으므로 여러 개의 암호 키를 활용하여 데이터 전송 상황에 맞게 랜덤으로 사용하는 방

식을 택해야 한다. 해양통신망에서는 해상 안전, 재난 구조 등 노드의 안전에 관련된 응용이 매우 중요하기 때문에 만약 악의적인 노드가 메시지를 도청한다 해도 그 내용을 알 수 없도록 하고 임의로 수정할 수 없도록 해야만 한다.

셋째, 선박의 위치 및 경로 익명성을 보장해야 한다. 익명성이란 망에 참여하는 개체들의 비밀성을 보장하기 위한 것으로 공격자에게 정보의 수집을 제한하도록 한다[35]. 익명성은 외부 공격자의 침입을 막는 것 외에도 비밀성 보호에 대한 관심 및 요구가 증가함에 따라 필요성이 커지고 있는데 따른 것이며, 익명성을 보장하려는 연구 활동 또한 활발하다. 위치 익명성은 공격자와 망 구성 노드가 경로배정 경로 탐색 과정 중에 얻을 수 있는 어떤 정보로도 인접노드나 목적지 노드의 위치, 경로의 홉 수 등을 알아 낼 수 없어야 한다는 것이다. 또 경로 익명성은 패킷의 근원지와 목적지 그리고 패킷 경로 내에 있는 중간 노드들은 전달되는 패킷의 경로를 구성하는 노드를 파악할 수 없어야 한다는 것이다.

5. 결 론

본 논문에서는 여러 다중 홉 이동 무선망의 특징과 그에 따른 보안 취약점을 알아보고 보안 경로배정과 관련된 최근 연구를 살펴보았다. 여러 다중 홉 이동 무선망은 기본적으로 MANET의 특성을 따르지만 노드의 특성이나 주된 응용에 따라 서로 다른 특성을 보였다. 제안한 해양통신망의 경우 MANET과 같이 노드는 선박 내 통신 장치가 되고 중앙 통제 없이 노드 간 링크를 형성하여 통신망을 형성할 수 있고 VANET처럼 이동 경로가 정해져 있다. 하지만 MANET의 노드 특성과는 다르게 육상의 고정 노드와 같이 자원이 풍부하고 VANET과는 다르게 이동 속도가 크게 빠르지 않고 위상 변화도 빈번하게 일어나지 않는다.

해양통신망의 특성과 앞서 살펴본 여러 다중 홉 이동 무선망의 보안 취약점 등을 고려하면 출항 전 인증을 위한 정보를 부여받고 각 노드 단위로 이미 알고 있는 경로 상의 노드를 대상으로 인증을 수행하면 노드 간 신뢰성을 구축할 수 있고, 선박의 위치 및 경로 익명성을 보장하여 공격자에게 정보 수집을 제한하도록 할 수 있다. 인증과 익명성은 상호 대립되는 개념이므로 상호 보완하는 보안 구조에 대한 적절한 기준을 찾는 것이 중요하다.

후 기

본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음. [2008-F-046-01, E-Navigation 대응 IT-선박 융합핵심기술 개발]

참고문헌

[1] David E. Culler, "Wireless Sensor Network - the Next IT Revolution", KES 2004, October 2004.

[2] Ian Akyildiz, Xudong Wang, Weilin Wang, "Wireless Mesh Networks : A Survey", Elsevier computer Networks, Vol. 47, No. 4, pp. 445~487, March 2005.

[3] L. Jun, et al, "A Survey of Inter-Vehicle Communication", School of Computer and Communication Sciences. EPFL, CH-1015 Lausanne, Switzerland Technical Report IC, 2004.

[4] Shin-Lin Wu, Yu-Chee Tseng, "Wireless Ad Hoc Networking", Auerbach Publications(2007), pp. 506-533, 2007.

[5] 권태경, 신수연, 박상호, 박태진, "무선 센서 네트워크 보안", 한국통신학회지, 제23권 제9호, pp. 88-102, September 2006.

[6] Yi-ch, Hu and A.Perring, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security And Privacy, special issue on Making Wireless Work, Vol2, No.3, pp. 28-39, 2004.

[7] 김명일, 신수미, "이동 Ad-hoc 네트워크 환경

에서의 적응형 네트워크 토폴로지 구성", 정보과학회 가을 학술대회 논문집, 제31권 제2호, pp.217-219, October 2004.

[8] Shin-Lin Wu, Yu-Chee Tseng, "Wireless Ad Hoc Networking", Auerbach Publications, pp.301~302, 2007.

[9] Y. Seung and P. Naldurg and Robin Kravets, "Security-Awares Ad Hoc Routing for Wireless Networks", In Proceedings of MobiHOC, October 2001.

[10] 한인성, 유황빈, "Ad Hoc 네트워크 라우팅 보안을 위한 다중경로 기반의 MP-SAR 프로토콜", 한국통신학회 논문지 제33권, 제5호, pp. 260-267, 2008.

[11] 채동현, 한규호, 임경수, 안순신, "센서 네트워크의 개요 및 기술동향", 정보과학회지 제22권 제12호, pp. 5-12, 2004.

[12] N. Nasser and Y.Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications, Vol. 30, No. 11, pp. 2401-2412, September 2007.

[13] S. Lee, Y. Choi, "A secure alternate path routing in sensor networks", Computer Communications, Vol. 30, No. 1, pp. 153-165, 2006.

[14] 권태경, 이정근, 김원호, 조대형, "무선 메쉬 네트워크 소개: 링크간 관계 측정 및 처리율 분석을 중심으로", 정보과학회지 제24권, 제12호, pp. 107-114, 2006.

[15] 이용, 이구연, "무선 메쉬 네트워크 구축 및 보안 기술 현황", 정보보호학회지 제18권, 제2호, pp. 40-48, 2008.

[16] K. Sanzgiri, D. Laflammen, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol.23, No. 3, pp. 598-610, 2005.

[17] P. Papadimitrator and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", in Proc. the SCS communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), pp. 193-204, San Antonio, TX, 2002.

[18] 이규환, 이주아, 김재현, "무선 메쉬 네트워크의 패스워드 기반 인증 프로토콜", 대한전자공학회 전자공학회 논문지, pp. 54-62, 2007.

[19] 이상선, "H2-2 Networking for Inter-Vehicle Communication", KRnet 2008 the 16th Korea Internet Conference, pp. 770-780, 2008.

[20] Charles Harasch, Andreas Festag, Panos Papadimitratos, "Secure Position-Based Routing for VANETs", Vehicular Technology Conference, pp. 26-30, 2007.

[21] 최재덕, 정수환, "빠른 이동성을 지원하는 VANET 환경의 핸드오버 인증 프로토콜", 대한전자공학회, 전자공학회 논문지, pp. 30-39, 2008.

[22] Anand R. Prasad, Neeli R. Prasad, "802.11 WLANs and IP Networking: security, QoS, and mobility", ARTECH HOUSE, pp. 55-60, 2005.

[23] C. L. Tan, Pink and K. M. Lye, "A Fast Handoff Scheme for Wireless Networks", Proceedings of the 2nd ACM International Workshop on Wireless Mobile Multimedia, pp. 83-90, 1999.

[24] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화동향 및 전망", 전자통신동향분석 제18권, 제4호, pp. 36-46, 2003.

[25] 권정호, 박종태, "IEEE 802.11 무선랜에서 고속 이동성 지원을 위한 사용자 사전 인증 기법", 전자공학회논문지 제44권 TC편 제10호, pp. 191-200, 2007.

[26] Anand R. Prasad and Neeli R. Prasad,

"802.11 WLANs and IP Networking: security, QoS, and mobility", ARTECH HOUSE, pp. 49-54, 2005.
[27] 윤철식, 차재선, "WiBro/Mobile-WiMAX 표준 개요", 정보과학회지 제25권, 제4호, pp. 5-14, 2007.
[28] 김영일, 안지환, 황승구, "WiBro와 WiMax 기술", 한국통신학회지 (정보통신) 제22권, 9호, pp. 112-127, 2005.
[29] 손태식, 최욱, 최효원, "Mobile WiMax 보안 이슈와 해결 방안", 한국통신학회지 (정보와통신) 제24권, 제11호, pp. 5-13, 2007.
[30] IEEE 802.16's Relay Task Group, http://www.802wirelessworld.com
[31] IEEE Standard 802.16j-2007, "IEEE Standard for Local and metropolitan area network Part 16:Air Interface for Fixed and Mobile Broadband Wireless Access Systems", 2007.
[32] 손주영, 문성미, "해상이동통신망을 위한 복합형 항로기반 라우팅 프로토콜", 「한국해양대학교 부설 산업기술연구소 연구논문집」, 제23권 pp. 137-140, 2006.
[33] M. Abolhasan, T. Wysocki, E. Dutkiewicz "A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks 2(2004), Elsevier, pp. 1-22, 2004.
[34] 김영세, 이정우, 한진희, 신진아, 전성익, "무선 네트워크 연동 보안 기술 동향", [ETRI]전자통신동향분석 제20권, 제1호, 2005.
[35] 백정하, 김범한, 이동훈, "그룹서명에 기반한 익명성을 제공하는 애드 혹 라우팅 프로토콜", 정보보호학회 학회지 제17권, 제5호, pp. 15-25, 2007.

저 자 소 개

문성미(文成美)

1998년~2002년 한국해양대학교 자동화정보공학부 졸업, 2002년~2004년 한국해양대학교 컴퓨터공학과 졸업(석사), 2005년~한국해양대학교 컴퓨터공학과 박사과정 재학, 관심분야는 해양정보통신망, MANET, VANET, WMN

손주영(孫周永)

1981년~1985년 서울대학교 계산통계학과 졸업, 1991년~1993년 서울대학교 컴퓨터공학과 졸업(석사), 1993년~1997년 서울대학교 컴퓨터공학과 졸업(박사), 1985년~1998년 LG전자(주) 책임연구원, 1998년~현재 한국해양대학교 컴퓨터공학과 교수. 관심분야는 해양정보통신망, MANET, VANET, WMN.
e-mail 주소 : mmlab@hhu.ac.kr