LEACH 프로토콜에 적합한 명세기반 침입탐지 기법

정회원 이 윤 호*°, 강 정 호**, 이 수 진*

A Specification-based Intrusion Detection Mechanism for LEACH Protocol

Yunho Lee*°, Jungho Kang**, Soojin Lee* *Regular Members*

요 약

무선통신기술과 임베디드 기술의 발달로 무선 센서네트워크는 다양한 분야에서 활발하게 응용되고 있기는 하지만, 자원제약적 특성을 가지는 센서 노드와 네트워크 자체의 특성들로 인해 다른 네트워크에 비해 많은 보안 취약점들을 가지고 있다. 이러한 보안 문제를 해결하기위해 암호화나 인증 등의 전통적 보안 메커니즘을 활용할 수 있지만, 잠식된 노드에 의한 공격에는 전통적 보안 메커니즘만으로는 적절히 대응할 수 없다. 따라서 무선 센서네트워크의 적절한 보안환경을 위해서는 2차적 보안 메커니즘이 필요하며, 이는 침입탐지 시스템이 고려될 수 있다. 이에 본 논문에서는 무선 센서네트워크의 클러스터링 라우팅 프로토콜인 LEACH(Low Energy Adaptive Clustering Hierarchy)를 대상으로 하여 안전하고 신뢰성 있는 네트워크를 형성할 수 있도록 해 주는 명세기반의 침입탐지 기법을 제안한다.

Key Words : 침입탐지, LEACH, specification, WSN, 보안

ABSTRACT

With the improvement of wireless communication and embedded technology, WSN is used at various fields. Meanwhile, because WSN is resource constrained, it is more vulnerable than other networks. To solve the security problem of WSN, we can use the traditional secure mechanism like as cryptography and authentication. But the traditional secure mechanism is not enough for all security issues that may be happened in WSN, especially attacks caused by the compromised node. So, we need the IDS as the second secure mechanism for WSN. In this paper, we propose the Specification-based Intrusion Detection Mechanism that makes LEACH, which is one of the clustering routing protocol for WSN, more reliable and safety.

Ⅰ. 서 론

무선 센서네트워크는 일반적으로 낮은 비용과 자원 제약의 특성을 갖는 소형 센서 노드들로 구성되는 self-organized 무선 네트워크 시스템을 말하는 것으로 최근 그 활용이 증가하고 있는 추세이다.

무선 센서네트워크는 일반적으로 적 공격에 강력하게 대응할 수 있는 장비에 장착되어 사용되지 않으며, 위험지역에 적절한 관리 없이 배치되기 때문에 적에게 쉽게 포획되고 자신을 정보를 쉽게 노출한다. 뿐만 아니라 잠식된 노드의 경우에는 해당 노드를 이용한 다양한 비정상적 공격을 수행할 수 있게 된다. 따라서 무선 센서네트워크에서 보안 문제는 네트워크의 성능 문제만큼이나 중요하게 다뤄져야 한다.

암호화 및 접근 제어 그리고 인증 서비스 등의 전통적인 보안 메커니즘은 무선 네트워크의 보안 문제를 어느 정도 해결해 줄 수 있다. 그렇지만 전

* 국방대학교 국방정보체계학과 (yunholee@gmail.com, cyberkma@gmail.com), (°: 교신저자)
** 아주대학교 NCW학과(kjhsea@ajou.ac.kr)
논문번호 : KICS2011-08-377, 접수일자 : 2011년 8월 29일, 최종논문접수일자 :2012년 1월 27일

통적 보안 메커니즘만으로 무선 네트워크 환경에서 발생하는 모든 공격에 적절하게 대응할 수는 없다. 따라서 무선 네트워크에서 적절한 보안 환경을 유지하기 위해서는 전통적 보안 메커니즘과 더불어 추가적인 2차적 보안 시스템이 필요하며, 이 2차적 보안 시스템으로는 지속적으로 네트워크를 모니터하며, 시스템의 공격상태 여부를 판단할 수 있는 침입탐지 시스템이 고려될 수 있다.

침입탐지 기법은 침입탐지 방법에 따라 비정상 행위 탐지(Anomaly Detection), 오용 탐지(Misuse Detection), 명세기반 탐지(Specification-based Detection) 등 3가지로 구분된다.

비정상 행위 탐지 기법은 Training Phase를 통해 자료를 축적하여 이를 기초로 정상 행위(범위)를 정의하고 이를 실제 시스템 동작과 비교하여 그 차이를 기준으로 공격을 탐지하는 기법이다. 따라서 알려지지 않은 공격에 대한 탐지가 가능하나 정상노드의 예기치 않은 오류로 발생 가능한 문제까지 공격으로 식별하여 오탐율이 높은 편이다. 오용탐지 기법은 알려진 공격의 특성과 수집한 데이터를 비교하여 서로 일치할 경우 공격 행위로 탐지하는 방법이다. 이 기법의 경우 알려진 공격에 대한 일치여부를 판단하기 때문에 알려진 공격에 대한 탐지율이 매우 높다는 장점을 가지고 있지만, 반면에 알려지지 않은 공격에 대해서는 탐지가 어렵다는 단점을 가지고 있다. 명세 기반 탐지 기법은 중요 객체들의 정상 동작을 직접적으로 보안 명세형태로 개념화 시켜, 이를 해당 객체들의 실제 동작과 비교하는 기법이다. 이 기법은 정상 동작(절차) 명세를 기준으로 객체가 올바르지 않은 동작(절차)을 수행할 경우 이를 침입으로 식별하기 때문에 알려지지 않은 공격에 대한 탐지가 가능할 뿐만 아니라 오탐율도 낮은 장점을 가지고 있다.

본 논문에서는 무선 센서네트워크의 라우팅 프로토콜에 적합한 침입탐지구조를 제시한다. 이 때 적용 대상 프로토콜은 무선 센서네트워크의 클러스터링 프로토콜인 LEACH를 사용하며, 탐지 기법은 명세 기반 탐지 기법을 적용한다.

이를 위해 본 논문에서는 LEACH 프로토콜을 분석하여 프로토콜의 보안상 취약점을 분석하고, 발생 가능한 이상 행위를 식별해 낸다. 침입탐지와 관련해서는 LEACH 프로토콜에 적합한 침입탐지 구조와 침입탐지 Agent모델을 제시한다. 그리고 이상 행위 탐지를 위해 필요한 조건이나 정책을 추가하여 확장된 프로토콜 명세를 제시할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 LEACH 프로토콜 및 관련연구에 대해 살펴본다. 3장에서는 LEACH 프로토콜에서 발생 가능한 이상 행위를 식별하고 이를 탐지하기 위한 명세 기반의 침입탐지 기법을 제시한다. 4장에서는 제안하는 침입탐지 기법에 대한 실험 및 분석 결과를 기술하고, 마지막으로 5장에서 향후 연구방향을 제시하고 결론을 맺는다.

Ⅱ. 배경지식 및 관련연구

2.1 LEACH 프로토콜

Heinzelman 등은 처음으로 에너지를 효율적으로 사용하기 위한 클러스터 기반의 라우팅 프로토콜인 LEACH를 제안하였다[1]. LEACH는 전체 노드들의 균등한 에너지 사용을 목적으로 하며, 전체 네트워크를 클러스터(cluster)라는 작은 지역으로 논리적으로 분할한다. 각 클러스터에는 헤더(Header)를 중심으로 구성되며, 헤더는 지역내 노드들의 통신 충돌을 회피하기 위한 TDMA(Time division multiple access) 스케줄을 생성 관리하고, 예하 노드들로부터 데이터 패킷을 수신 및 종합하여 베이스스테이션(Base Station)에게 전송하는 역할을 담당한다.

LEACH는 그림 1과 같이 형성 단계와 지속상태 단계로 나뉘어 동작한다.

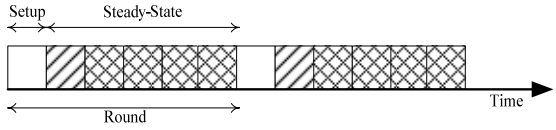

그림 1. LEACH 프로토콜 동작단계
Fig. 1. LEACH protocol phases

2.1.1 형성 단계(Setup Phase)

형성 단계는 3가지 절차로 구성되어 있다. 첫 번째 절차에서 노드들은 자가 선출 기법을 통해 스스로 해당 라운드에서 클러스터 헤더(CH: Cluster Header)가 될지를 결정한다. 스스로 선출된 클러스터 헤더 노드들은 광고 메시지를 브로드캐스트한다. 두 번째 절차에서는 광고 메시지를 받은 노드들은 가장 가까운 클러스터 헤더를 선택하여 참여 메시지를 보낸다. 세 번째 절차에서는 각 클러스터 헤더는 참여 메시지를 보낸 노드들을 자신의 멤버 노드로 뽑고, 확인 메시지와 지속상태 단계 동안에 쓰일 TDMA 스케줄을 브로드케스트 한다. 그림 2는 형성 단계를 통해 클러스터링된 LEACH 프로토콜 형상을 나타낸다.

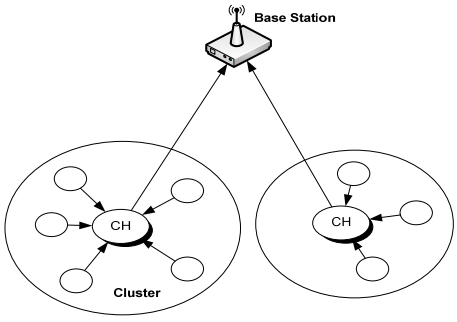

그림 2. LEACH 프로토콜 클러스터링
Fig.2. LEACH protocol clustering

2.1.2 지속상태 단계(Steady-State Phase)

지속상태 단계에서는 각각의 노드들이 패킷 충돌을 막기 위해 수신한 TDMA 스케줄에 따라 통신을 한다. 멤버 노드들은 자신의 전송 시간대가 오면 데이터를
클러스터 헤더에게 전송한다. 각 클러스터 헤더는 전송할 데이터의 양을 줄이기 위해 멤버 노드들로부터 수신한 데이터들을 사전에 정의된 퓨전 함수를 이용해 취합하고, 그 결과를 베이스스테이션에 전송한다.

이상의 전체적인 과정은 한 번의 라운드 동안 수행하며, LEACH 프로토콜은 네트워크 전체의 에너지 효율을 위해 클러스터 헤더를 번갈아 선출하는 재 클러스터링을 수행함으로써 라운드를 순차적으로 진행시켜 나간다.

2.2 관련 연구

센서 네트워크의 보안 강화와 관련한 연구는 대부분이 암호화된 키를 이용하여 보안 목표를 달성하는 전통적 메커니즘 중심으로 이루어졌다. LEACH와 관련해서도 마찬가지여서 LEACH의 보안문제를 개선하기 위해 제시된 기법들도 대부분이 키를 이용하여 안전한 통신채널을 구성하는데 중점을 두고 있다.

Oliveira 등은 안전한 클러스터링을 위해 LEACH에 Eschenauer 등이 제안한 임의의 키 사전 분배 방식[2]을 적용한 SecLEACH[3] 프로토콜을 제안하였다. SecLEACH 기법은 배포 전에 임의의 키 사전 분배 방식처럼 S개의 키들로 이루어진 키 풀과 키 id를 만들어 각각의 노드는 m개의 키들로 이루어진 키 링을 임의로 할당받는 방식을 채택하고 있다.

Banerjee 등은 SecLEACH 기법에서 일반 노드가 항상 가장 가까운 클러스터 헤더를 선택할 수도 없다는 문제점을 개선한 GS-LEACH를 제안하였다[4]. GS-LEACH에서는 그리드 기반의 센서 노드들의 배포를 가정한다. 즉 센싱 지역을 k개의 정사각형 모양의 그리드들로 나누고, n개의 센서 노드들을 각각의 그리드에 배포되도록 한다.

이상의 방법들은 정상적으로 암호키를 가지고 있는 센서 노드가 공격자에게 탈취되어 악의적인 노드 역할을 할 경우, 이에 대한 적절한 대응을 취할 수 없어 여전히 센서네트워크의 무결성 및 가용성에 관하여 보안 취약점을 가지고 있다. 따라서 무선 센서네트워크의 적절한 보안을 위해서는 암호키 방식이나 인증과 같은 전통적 암호 메커니즘 외에도 노드들의 행위 또는 수집된 정보를 통해 공격 여부를 판단하고, 대응할 수 있는 침입 탐지 시스템이 추가적으로 필요하다.

그래서 본 논문에서는 LEACH 프로토콜에 대하여 이러한 내부 공격에 대한 탐지와 대응이 가능한 적합한 명세 기반의 침입탐지 기법을 제시한다.

Ⅲ. LEACH 프로토콜을 위한 명세기반 침입탐지 기법

3.1 탐지 대상

3.1.1 LEACH 프로토콜 단계별 이상행위

LEACH 프로토콜은 크게 4단계로 구분된다. 각 단계별 공격 노드가 취할 수 있는 행위를 살펴보면 다음과 같다.

■ Advertisement Phase

Advertisement 단계에서는 각 노드가 자신이 헤더가 될 것인지를 결정하고 이를 일반 노드에게 광고를 하는 단계이다. LEACH 프로토콜에서는 헤더가 되었을 경우 일반 노드보다 네트워크에 대한 영향력이 크다. 이러한 이유로 만약에 공격노드가 헤더가 되었을 경우에는 해당 클러스터에 대한 다양한 공격이 가능하게 된다. 특히, 공격 노드가 지속적으로 헤더가 되는 경우에는 공격을 장시간 유지할 수 있으므로, 자신의 공격효과를 극대화 시킬 수 있다. 여기서 공격 노드가 헤더가 되는 경우는 LEACH 프로토콜 자체가 헤더 결정을 각 노드에게 맡기는 형태이기 때문에 이상행위로 볼 수 있는 것은 해당 라운드에서 헤더를 2회 이상 지속하는 것이다.

이 단계에서 공격노드가 취할 수 있는 또 하나의 행위는 자신의 헤더 정보를 광고할 때 필요이상의 강한 전파를 사용하는 것이다. 일반 노드들은 수신된 헤더 정보들 중에서 전파의 세기를 통해 자신과의 상대적 위치가 가까운 노드를 자신의 헤더로 선택하여, 참여 희망 메시지를 보내게 된다. 이 과정에서 공격 노드는 자신의 광고 메시지의 전파를 증폭하여 먼 거리

의 노드에게도 자신이 가까이 있는 것처럼 보이게 할 수 있고, 더 많은 노드들을 자신의 클러스터에 포함시켜 이후 자신의 공격 범위를 확대 할 수 있다. 추가적으로 먼 거리의 일반노드들이 자신이 선택한 클러스터 헤더 데이터를 전송하기 위하여 더 많은 에너지를 사용 하게 되어, 노드들의 수명을 단축시키는 문제를 야기 시킬 수 도 있다.

■ Cluster Set-Up

일반 노드들이 수신한 헤더 정보를 가지고 자신에게 적합한 헤더를 선택하여, 참여 희망 의사를 전달하는 단계이다. 이 단계에서 공격노드가 취할 수 있는 절차상 정상적이지 않은 행위로는 클러스터에 참여 의사를 보내지 않는 행위이다. 이 행위는 해당 노드의 센싱 지역에 대한 데이터를 누락시키는 결과를 가져온다.

■ Schedule Creation

참여 희망 노드 정보를 수신한 헤더가 참여 희망 노드 상황에 맞게 TDMA를 위한 스케줄을 만들어서 이를 전달하는 단계이다. 이 단계에서 공격을 위한 행위로는 헤더가 자신의 클러스터에 참여를 희망한 일반 노드들에게 참여 결정 응답의 의미를 가지는 TDMA 스케줄을 전달 해 주지 않는 행위가 있다. 이로 인해 해당 클러스터에 참여를 희망한 노드들은 자신의 정보를 전달 해 줄 수 없게 되고, 베이스스테이션는 해당 지역에 실제 정보를 수집할 수 없게 된다.

■ Steady-State Phase

실제로 데이터를 송수신 하는 단계로, 일반 노드에서 수집한 데이터를 헤더에게 보내고, 헤더는 수신된 정보를 조합하여 이를 베이스스테이션으로 전송한다.

이 단계에서 공격자가 일반 노드일 경우에는 데이터를 전송하지 않는 행위와 헤더의 정상적인 데이터 수집을 방해하기 위해 다른 노드들과 같은 시간대에 데이터를 전송하는 등의 충돌을 야기하기 위한 TDMA스케줄을 의도적으로 미준수하는 행위가 가능하다. 전자의 경우는 클러스터에 참여하지 않는 경우와 같이 해당 지역 정보 수집을 불가능하게 하는 공격이며, 후자의 경우는 다른 노드들과의 충돌을 야기 시켜 헤더의 정보 수집에 영향을 가하게 된다. 만약 이 공격이 지속된다면, 헤더의 기능을 수행하는 데 더 많은 시간과 자원을 사용하게 되어, 성능저하에 영향을 줄 수 있다.

공격자가 헤더인 경우에는 데이터를 베이스스테이션에 전송하지 않거나, 다른 곳으로 전송하여 데이터를 중간에서 가로챌 수 있다. 또한 실제 수집한 데이터의 조합이 아닌 공격 의도 맞게 가공한 잘못된 데이터를 전송할 수도 있다.

3.1.2 탐지 대상 행위

앞에서 살펴본 이상 행위 중에서 일반 노드의 클러스터 미 참여 행위는 해당 노드가 목적을 가지고 취한 행위인지, 아니면 에너지가 완전히 소모되어 동작을 안 하는 것인지 구별하기 힘들다. 따라서 단일 노드의 행위를 통해 이상 행위를 식별하는 것 보다 센서네트워크 성능 측면에서 허용하는 비동작 노드 비율을 정하고 이를 기준으로 하여 이 비율 내에서는 특정한 조치를 취하지 않고, 네트워크 성능에 치명적 영향을 주는 비율 이상으로 나타나는 경우에 네트워크 유지 여부를 고려하는 방법으로 문제를 해결해야 될 것으로 판단된다.

그리고 Steady-State 단계에서 헤더 노드와 일반 노드의 잘못된 데이터 전송 행위는 절차상의 이상 행위가 아니라 전송되는 데이터에 문제가 있는 것으로 본 논문의 목적인 절차의 정상적 명세를 기준으로 이상 행위를 식별하는 방법으로 탐지하기는 어렵다. 따라서 이 행위(공격)의 탐지를 위해서는 본 논문에서 제시하는 방법이 아닌 다른 방법이 필요로 하며, 이를 위한 방법으로는 통계적 추정 기법[5]과 SDAP(Secure Hop-by-Hop Data Aggregation Protocol)[6], RANSAC (RANdom SAmple Consensus)[7] 등을 사용할 수 있다.

데이터를 다른 곳으로 유출하는 행위는 정상적인 Omnidirectional 전파를 사용하는 경우와 Directional 전파를 사용하는 경우로 구분하였을 때, 정상적인 전파를 사용하는 경우는 자료를 유출하는 과정에서 데이터가 베이스스테이션까지 도달한다고 보면 이는 절차상에서는 아무런 문제가 없는 행위로, 본 논문에서 제시하는 기법으로는 탐지하는 것이 어렵다. 그리고 Directional 전파를 사용하는 경우에는 베이스스테이션으로 전파가 도달하지 않아 결국 데이터 미전송과 동일한 현상으로 나타난다. 따라서 이 경우에는 데이터 미전송으로 포함시켜 처리할 수 있다.

따라서 본 논문에서 제안하는 명세기반 침입탐지 기법은 앞에서 설명한 4가지 행위를 제외하고 표 1에서 보는 것과 같이 6가지 이상 행위만을 탐지 대상으로 하였다.

3.2 침입탐지

3.2.1 LEACH 프로토콜에 적합한 침입탐지 구조

본 논문에서 제시하는 침입 탐지 모델은 Wenke Lee 등이 제안한 분산/협동 침입 탐지 구조(Distributed and Cooperative Intrusion Detection Architecture)[8]

표 1. 탐지 대상 이상행위
Table 1. List of misbehaviors

Phase 구분	이상 행위	영 향
Advertisement	지속적 헤더	·지속적인 헤더로 자신의 클러스터에 대한 지속적 공격 가능
	강한 에너지 전송	·최대한 많은 노드를 자신의 클러스터에 포함시켜 공격 효과 확대 ·장거리 데이터 전송을 통해 노드의 에너지 소비 촉진
Schedule Creation	스케줄 미전송	·해당 CH를 선택한 일반 노드들에 대한 정상적인 동작 방해
Steady-State	스케줄 미준수	·CH의 데이터 수신 방해
	일반 노드 데이터 미전송	·해당 지역 감시정보 누락
	헤더 노드 데이터 미전송	·해당 클러스터의 자료 Drop

를 참조하였으나, 이 구조에서 고려된 MANET과 달리 센서네트워크에서는 베이스스테이션이라는 충분한 자원과 처리능력을 가지고 있는 신뢰성 높은 중앙 요소가 있어, 이 베이스스테이션을 중심으로 하는 탐지 구조를 구성하였다.

그림 3은 본 논문에서 제시하는 침입탐지 구조를 묘사한 것이다. 그림에서 보는 것처럼 클러스터 헤더를 포함한 일반 센서 노드들은 각자가 탐지한 이상 행위를 베이스스테이션으로 전송한다. 베이스스테이션은 각 노드에서 보내온 정보와 자신이 직접 탐지한 정보를 종합하여 공격 행위 여부를 결정하고 이를 각 노드에 전파하여 공격에 대한 대응을 지시한다.

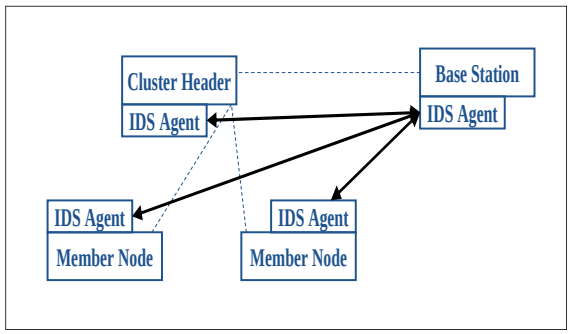

그림 3. 침입탐지 구조
Fig. 3. Structure of the intrusion detection technique

이 구조는 각 센서 노드에서는 침입 탐지 작업의 부하를 줄이고, 보다 자원에 여유가 있고 신뢰도가 높은 베이스스테이션에서 각 노드에 탐지한 정보를 통합하여, 침입 여부를 결정함으로써, 무선 네트워크의 기본적 침입 탐지 구조를 유지하면서 센서 노드의 수명을 좀 더 연장할 수 있으며, 보다 신뢰도 있는 탐지 결과를 가져 올 수 있다.

3.2.2 명세기반 탐지

(1) 이상행위 식별

본 논문의 탐지 대상인 6개 이상행위에 대한 절차를 통한 식별 방안은 다음과 같다.

■ 지속적 헤더 노드 유지

지속적 헤더 노드 유지는 기존의 헤더 노드 정보를 유지하고 이 정보와 현재 헤더 노드가 된 노드 정보를 비교하면 쉽게 식별해 낼 수 있다. 이를 위해 본 논문에서 제안하는 방법은 각 노드가 자신이 수신한 헤더 노드 정보를 별도로 저장하고, 새로운 헤더 노드 선정 주기마다 수신한 헤더 노드 정보와 저장된 자료를 비교한다. 만약 2회 이상 중복되는 헤더 노드가 있으면 이를 이상 행위로 식별한다.

■ 강한 에너지 전송

강한 에너지 전송 행위를 식별해내기 위해서는 자신이 수신한 헤더 노드들이 실제 자신과 근접해 있는지를 확인하는 절차가 필요하다.

이를 위해 본 논문에서는 그림 4에서 보는 것처럼 일반 노드가 헤더 노드 광고를 수신 후에 수신한 전파를 기준으로 거리를 산출하여 산출된 거리까지만 도달할 수 있는 적합한 세기로 참여 의사 메시지를 전송한다. 그런 후에 해당 헤더 노드에서 TDMA 스케줄 정보를 정상적으로 자신을 포함하여 보내온 경우에는 정상적인 노드로 판단하여 후속 절차를 수행한다. 그러나 TDMA 스케줄 정보가 되돌아오지 않거나, 수신한 TDMA 스케줄 정보에 자신이 포함되어 있지 않는 경우에는 해당 헤더 노드가 자신이 보낸 참여 의사 메시지를 수신하지 못한 것이고, 이는 결국 광고 메시지 전파의 세기가 비정상적인 것으로 판단하여, 이를 이상 행위로 식별해 낸다.

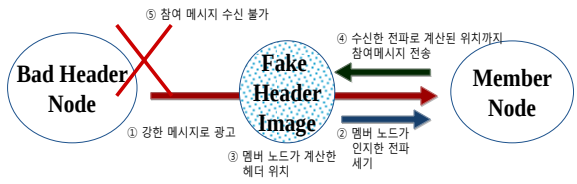

그림 4. 강한 에너지 전송 행위 탐지 방법
Fig. 4. Strong signal misbehavior detection method

■ 스케줄 미전송

일반 노드가 클러스터 참여 의사 메시지를 헤더 노드에 전송하고, 일정 시간 후 까지 TDMA 스케줄 메시지를 수신하지 못하였을 경우에는 그 자체를 이상 행위로 식별할 수 있다.

■ TDMA 스케줄 미준수

일반 노드 중에 클러스터 헤더 노드의 정보 수집을 방해하기 위해 TDMA 스케줄과 상관없이 자료를 전송하는 경우에는 헤더 노드가 가지고 있는 TDMA 스케줄 정보와 실제로 자료를 보내온 노드 정보의 노드 ID를 비교하여 쉽게 이상 행위를 식별할 수 있다. 만약에 자료를 전송한 노드들 중에 해당 시간대가 아닌데도 자료를 전송한 경우에 이를 이상 행위로 식별한다.

■ 일반 노드의 데이터 미전송

일반 노드가 헤더 노드에게 데이터를 전송하지 않는 경우에는 헤더 노드가 가지고 있는 자신의 클러스터 멤버 노드 정보를 기준으로 하여 해당 전송 시간에 자료 전송이 이루어지지 않는 노드를 이상 행위 노드로 식별한다.

■ 헤더 노드의 데이터 미전송

헤더 노드가 데이터를 전송하는 경우에는 주변의 일반 노드가 헤더 노드가 발송하는 전파를 감지 할 수가 있다. 따라서 만약에 일반 노드가 데이터를 헤더 노드로 전송한 후에 자신의 다음 전송 주기까지 헤더 노드에서 발송되는 전파를 감지하지 못하면, 헤더 노드가 데이터를 베이스스테이션으로 전송하지 않은 것으로 판단하고 이를 이상 행위로 식별한다.

(2) 이상행위 탐지를 위한 확장된 LEACH 프로토콜 명세

LEACH 프로토콜의 일반 상태 전의는 4단계로 구성할 수 있으며, 각 단계에서 다음 단계로 넘어가는 조건은 매우 간단하여, LEACH의 기본 프로토콜에서는 상태 전의 과정에서 이상 행위를 탐지하는 것은 불가능하다고 볼 수 있다. 그래서 본 논문에서는 논문의 목적인 프로토콜 절차상에서 이상 행위 탐지가 가능하도록 하기위해 상태 전의와 전의 조건을 좀 더 구체화하여 기존 프로토콜을 확장시켰다.

그림 5는 본 논문에서 제안하는 침입탐지를 위한 LEACH 프로토콜의 확장된 명세를 상태 전의 다이어그램으로 표현한 것이다. 그림에서 보는 바와 같이 제안하는 명세는 각 Status 별로 해당 Status에서 발생 가능한 이상 행위를 식별해내기 위해 필요한 절차와 이상 행위를 처리하기 위한 Status를 추가하였다.

Ⅳ. 실험 및 분석

4.1 실험 환경

NS-2 시뮬레이터를 이용, 실험을 위하여 100m × 100m 크기의 가상 무선 센서네트워크 환경을 구현하였다. 이 가상의 필드에는 총 100개의 센서 노드를 배치하였고, 하나의 베이스스테이션을 구현하였다.

노드의 클러스터 헤더 비율은 클러스터 형성 20주기를 기준으로 평균 5% 비율로 선정되도록 하였으며, 실제와 유사한 환경을 구현하기 위해 데이터 전송 주기 1000라운드 당 평균 0.3%내의 비율로 자연적 오류 노드가 발생토록 구현하였다. 이상행위 및 공격행위 구현과 관련해서는 구현된 100개의 노드 중 임의의 노드를 선정하여 실험하고자 하는 행위를 수행토록 구현하였다.

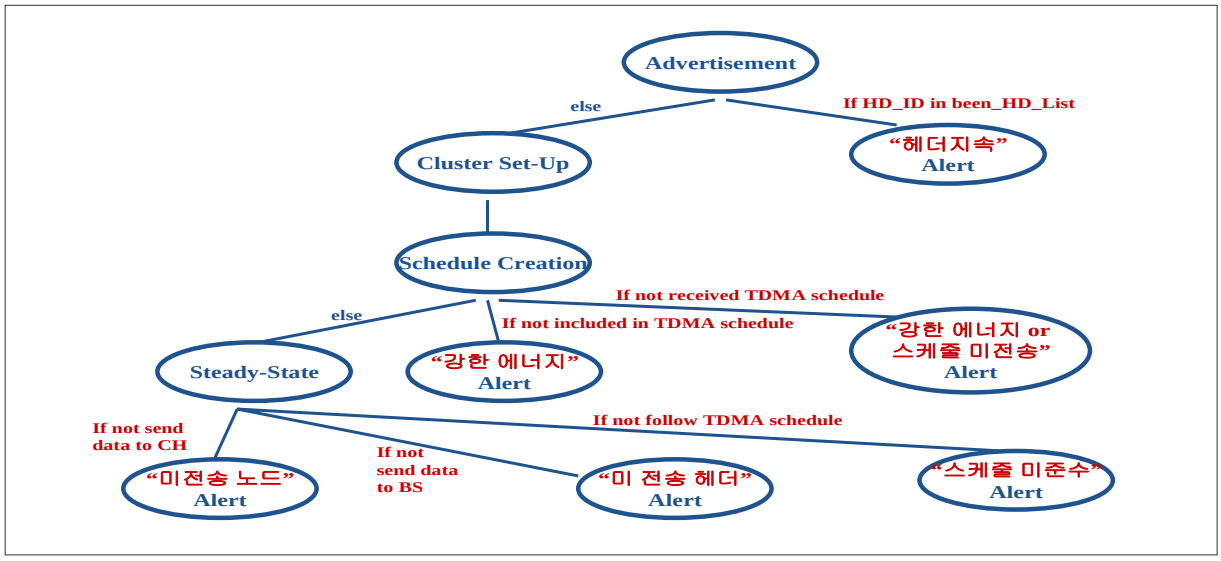

그림 5. 확장된 LEACH 프로토콜 상태 전이 다이어그램
Fig. 5. State Transition Diagram of Extended LEACH Protocol Specification

4.2 성능 분석

그림 6은 공격이 없는 상태에서 일반 LEACH 프로토콜의 데이터 전송율과 침입탐지 기법이 적용된 LEACH 프로토콜의 데이터 전송율을 비교한 결과이다. 그림에서 보는 바와 같이 본 논문에서 제안하는 침입탐지 기법이 기존 LEACH 프로토콜의 데이터 전송율에 영향을 주지 않는다는 것을 실험에서 보여준다.

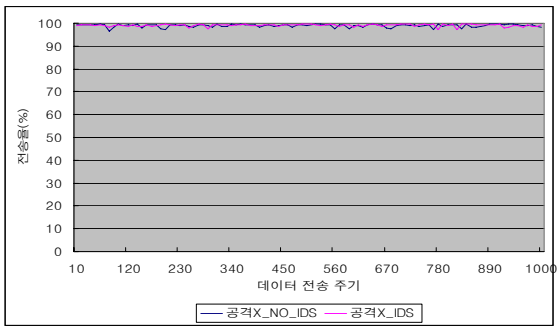

그림 6. 공격 없는 상황에서의 IDS 적용 전과 적용 후 전송율 비교
Fig. 6. Transmission rate comparison before and after implementing the IDS (without attack)

표 2. 침입탐지시스템 적용에 따른 데이터 전송 오버헤드
Table 2. Message transmission overhead caused by the IDS

차수 / 구분	1회	2회	3회	4회	5회	6회	7회	8회	9회	10회
경고 메시지	374	250	298	285	441	593	274	492	370	291
공격 처리	6	6	2	1	10	5	0	5	3	3
추가 패킷	974	850	498	385	1441	1093	274	992	670	591
전체 패킷	121000									
패킷 증가율 (%)	0.8	0.7	0.4	0.3	1.2	0.9	0.2	0.8	0.5	0.5

차수 / 구분	11회	12회	13회	14회	15회	16회	17회	18회	19회	20회
경고 메시지	569	526	348	443	181	239	385	308	363	209
공격 처리	9	4	5	3	0	4	3	6	1	2
추가 패킷	1469	926	848	743	181	639	685	908	463	409
전체 패킷	121000									
패킷 증가율 (%)	1.2	0.8	0.7	0.6	0.2	0.5	0.6	0.8	0.4	0.3

표 2는 침입탐지 기법 적용에 따른 패킷 증가 현황이다. 표에서 보는 바와 같이 제안하는 침입탐지 기법을 추가함으로 인해 발생하는 패킷 전송의 오버헤드는 0.2%에서 1.2%사이로 발생하였다. 이는 암호학적 기반의 SecLEACH의 최소 오버헤드가 20%인 이상인 점을 감안할 때 통신비용면에서 효율적으로 침입탐지를 수행한다고 판단할 수 있다.

표 3은 본 논문의 탐지 대상 이상행위에 대한 탐지율을 보여준다. 표에서 보는 바와 같이 모든 대상 행위에 대하여 90%이상의 높은 탐지율을 보여주고 있다.

표 2. 이상행위별 탐지율
Table 3. Detection rate of misbehaviors

	이상 행위1	이상 행위2	이상 행위3	이상 행위4	이상 행위 5	이상 행위6
탐지율 (%)	100	93.5	94	99.9	99.85	99.9

※ 이상행위 1 : 지속적 헤더 유지
이상행위 2 : 강한 에너지 사용 또는 TDMA 스케줄 미전송
이상행위 3 : 강한 에너지 사용
이상행위 4 : TDMA 스케줄 미전송
이상행위 5 : 데이터 미전송(멤버 노드)
이상행위 6 : 데이터 미전송(헤더 노드)

헤더 노드의 이상행위인 이상행위 2, 3, 6에서 오탐이 나타나는 이유는 이상행위 헤더 노드가 자신의 멤버 노드를 가지고 있지 않거나, 멤버 노드를 가지고 있으나 그 수가 적고 해당 노드의 경고 메시지가 전송 오류에 의해 베이스스테이션 까지 도달하지 못하는 경우가 발생 가능하기 때문이다. 그리고 멤버 노드의 이상행위인 이상행위 4, 5에서 오탐이 발생하는 이유는 클러스터 형성과정에서 이상행위 예정노드의 참여의사가 전송 오류에 의해 헤더 노드까지 전달되지 않아 클러스터에 참여되지 않은 상태에서 이상행위를 수행하여 탐지할 노드가 없는 상황이나, 이상행위를 탐지한 헤더 노드의 경고 메시지가 전송 오류에 의해 베이스스테이션까지 도달하지 못하는 상황이 발생할 수 있기 때문이다.

위 세 실험 결과를 살펴보면, 본 논문에서 제안하는 침입탐지 기법은 그 적용으로 인해 발생하는 프로토콜의 성능감소나, 추가적인 비용은 적은 반면에 탐지 대상행위에 대한 탐지율은 매우 높은 수치를 보여주는 것을 알 수 있다. 따라서 본 침입탐지 기법을 무선 센서네트워크에 적용했을 때 기존 프로토콜의 기능을 비슷한 수준에서 유지하면서, 침입 탐지에 대한 높은 성능을 보여 줄 것을 기대할 수 있다.

4.3 주요 공격 탐지 결과

LEACH 프로토콜은 클러스터 기반의 무선 센서네트워크 라우팅 프로토콜로 클러스터 헤더 노드에 의한 공격은 그 피해가 매우 클 것을 예상할 수 있다. 본 논문에서는 헤더 노드 공격으로 인해 네트워크에 발생하는 현상과 영향, 그리고 제안하는 침입탐지 기법을 적용했을 때 이에 대응하여 나타나는 현상과 효과를 검증하기 위해 탐지 대상 이상행위 중 헤더 노드와 관련된 행위를 기반으로 하는 3가지 공격 시나리오를 구성하여 시험을 실시하였다.

본 실험에서 이상행위 탐지 후 침입으로 최종 결정하는 기준이 되는 Threshold 값은 이상행위 성격에 따라 반복회수 2~3회 사이에서 임의로 선택하였다. 본 실험에서 사용한 Threshold 값은 최적화된 값은 아니다. Threshold를 낮출 경우에는 공격 지속시간이 더 짧아지고 조기에 정상으로 복귀할 수 있기 때문에 요구되는 보안 수준에 따라 적절히 조정할 필요가 있다.

4.3.1 공격 시나리오 #1

첫 번째 공격 시나리오는 하나의 공격 노드가 지속적으로 헤더 노드가 되면서 강한 에너지로 자신의 헤더 노드 정보를 광고하여 클러스터를 형성한 후에 멤버 노드로부터 수신한 데이터를 베이스스테이션으로 보내지 않고 드롭하는 경우이다. 이 공격에 의한 전송율 변화는 그림 7에서 보는 바와 같다. 데이터 전송율은 공격 노드의 전송 파워에 따라 달라지어 파워가 강하면 강할수록 공격에 영향을 받는 노드가 증가하여 전체 네트워크의 전송율은 낮아지게 된다. 이러한 공격은 클러스터 형태의 무선 센서네트워크에서 발생할 수 있는 가장 심각한 공격 형태라고 할 수 있다.

그림 8은 제안하는 침입탐지 기법을 적용한 상태에서 이 공격이 일어났을 때의 실험 결과이다. 공격 초기에 침입 상태를 탐지한 후에 바로 정상 수준의 데이터 전송율로 회복하는 것을 확인할 수 있다. 이는 제안하는 침입탐지 기법이 시나리오 #1 공격에 효과적으로 대응할 수 있음을 의미한다.

4.3.2 공격 시나리오 #2

공격 노드가 정상적으로 헤더 노드가 되어 강한 에너지로 자신의 헤더 노드 정보를 광고한 후에 참여 의사를 밝힌 노들에게 TDMA 스케줄을 전송하지 않는 경우이다. 이 공격은 결국 TDMA 스케줄을 전송받지 못한 일반 노드들을 네트워크에서 배제시키는 효과를 가져 온다.

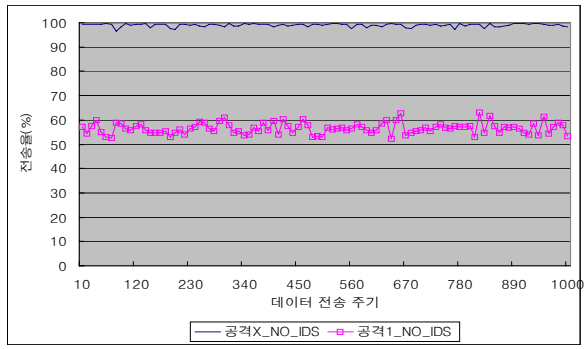

그림 7. 시나리오 #1 공격 실험 결과
Fig. 7. Simulation result of attack scenario #1

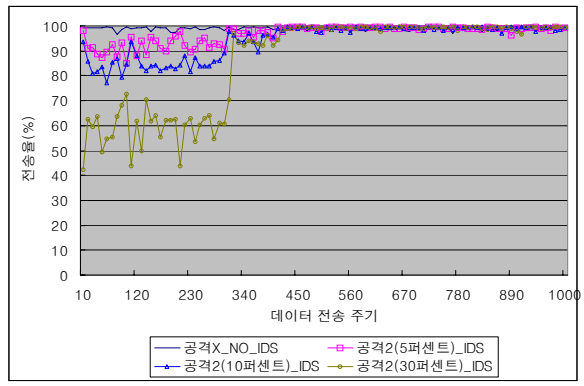

그림 8. 침입탐지 기법 적용 후 시나리오 #2 공격 실험 결과
Fig. 8. Simulation result of attack scenario #1 with IDS

그림 9는 각각 5%, 10%, 30%의 공격 노드를 적용하여 반복적으로 실험한 결과를 보여 주고 있다. 그림에서 알 수 있듯이 공격 노드가 5%인 상황에서는 그 피해가 미약하지만, 30%인 환경에서는 그 피해가 현저하게 증가한다.

그림 10은 침입탐지 기법을 적용한 환경에서 공격을 수행한 결과를 보여 준다. 침입탐지 기법을 적용한 상태에서는 공격 후 일정 시간 후에 데이터 전송율을 정상상태로 복귀시킨다. 이 때 공격 상태가 일정 기간 지속되는 이유는 침입탐지 기법이 이상 행위를 탐지 후 공격행위로 최종 결정하기 위해 Threshold까지 도달하는데 시간이 소요되기 때문이다.

4.3.3 공격 시나리오 #3

공격 노드가 정상적으로 헤더 노드가 되어 정상적인 에너지로 자신의 헤더 노드 정보를 광고하고 클러스터를 형성한 후에 멤버 노드의 데이터를 미전송시키는 공격이다. 그림 11에서 보는 바와 같이 공격으로 인해 나타나는 현상은 시나리오 #2와 유사하다. 그러나 시나리오 #2와 다른 점은 데이터 전송율이 시나리오 #3

이 상대적으로 더 높게 나타난다. 즉, 공격의 영향이 시나리오 #2가 시나리오 #3 보다 더 크다는 것이다. 이러한 차이가 나타나는 이유는 시나리오 #2에서의 공격 노드는 보다 큰 에너지를 사용하여 자신의 정보를 광고함으로써, 보다 많은 멤버 노드를 확보할 수 있지만 시나리오 #3에서는 정상적으로 헤더 노드가 되기 때문에 시나리오 #2에 비해 상대적으로 멤버 노드 수가 적어 공격의 영향이 적게 나타나게 되는 것이다.

그림 12는 제안하는 침입탐지 기법을 적용했을 때 나타난 실험 결과 이다. 그림에서 보면 정상으로 복귀하는 시간이 시나리오 #2에 비해 빠르게 나타난다. 그 이유는 이상 행위를 탐지할 수 있는 주기가 시나리오 #2는 클러스터 형성 주기인데 반해 시나리오 #3은 데이터 전송 주기이기 때문이다. 즉, 1회 클러스터 형성 후 여러번의 데이터 전송이 일어나기 때문에 공격행위 결정을 위한 Threshold까지 도달하는 시간이 시나리오 #3이 시나리오 #2에 비해 상대적으로 적게 걸리는 것이다. 그림에서 보는 바와 같이 이 공격에 대해서도 제안하는 침입탐지 기법이 효과적으로 대응하는 것을 알 수 있다.

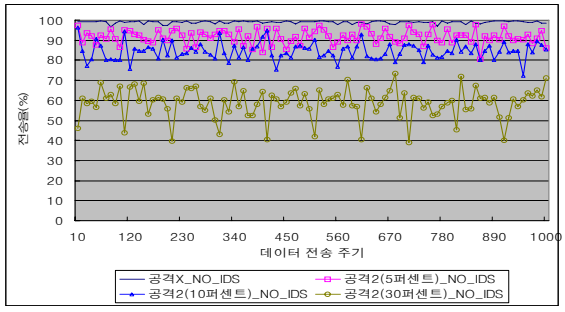

그림 9. 시나리오 #2 공격 실험 결과
Fig. 9. Simulation result of attack scenario #2

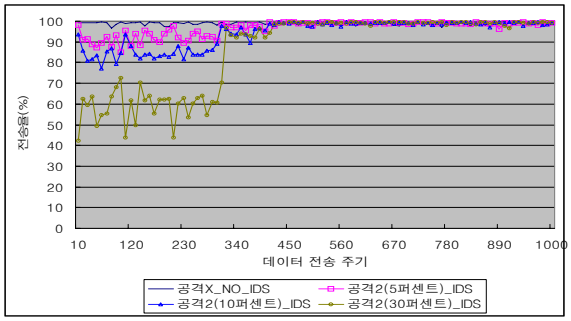

그림 10. 침입탐지 기법 적용 후 시나리오 #2 공격 실험 결과
Fig. 10. Simulation result of attack scenario #2 with IDS

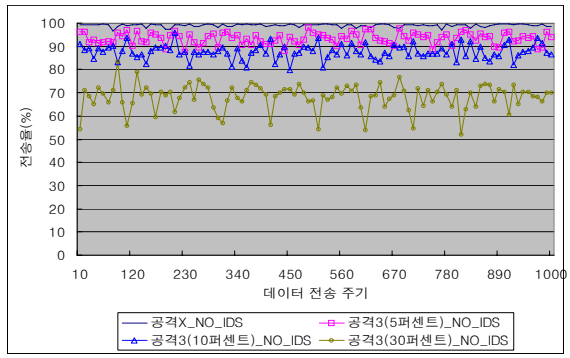

그림 11. 시나리오 #3 공격 실험 결과
Fig. 11. Simulation result of attack scenario #3

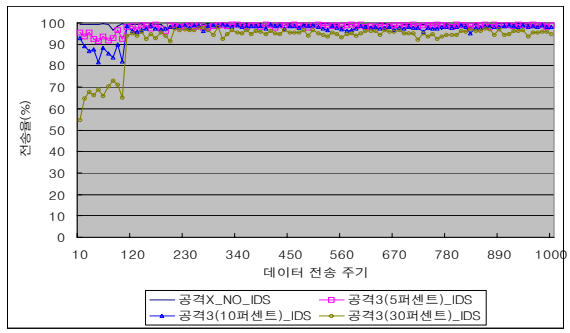

그림 12. 침입탐지 기법 적용 후 시나리오 #3 공격 실험 결과
Fig. 12. Simulation result of attack scenario #3 with IDS

V. 결 론

본 논문에서는 LEACH 프로토콜에 적합한 명세기반 침입탐지 기법을 제안하였다. 이를 위 먼저 LEACH 프로토콜의 동작 과정을 분석하여 절차상에서 발생 가능한 이상행위를 식별하였고 이중 실제 침입탐지가 필요하고, 명세기반 침입탐지가 가능한 이상행위를 탐지 대상으로 선정하였다. 그리고 침입탐지 기법과 관련해서는 클러스터 구조를 제안하여, 효율적이고 신뢰도 높은 침입탐지 기법을 구현하는데 초점을 두었다. 또 분석된 이상행위 탐지를 위해서 LEACH 프로토콜의 확장된 명세를 정의하였으며, 이를 기반으로 하는 명세기반 침입 탐지 기법을 제안하였다.

성능 평가 결과, 제안하는 침입탐지 기법은 탐지 대상 이상행위에 대한 높은 탐지율을 보이면서도 낮은 수준의 오버헤드만을 발생시키고, 기본 LEACH 프로토콜과 유사한 데이터 전송율을 유지함을 보여주어, 제안하는 침입탐지 기법이 LEACH 프로토콜에 적합하고 적용이 가능한 기법임을 입증하였다.

본 연구를 통해, 불확실한 환경에서 운영되는 무선 센서네트워크에 적합한 침입탐지 기법으로 네트워크의

라우팅 프로토콜에 대한 명세기반 침입탐지 기법이 효용성이 클 것이라는 것을 알 수 있었다. 따라서 향후 연구로는 더 다양한 라우팅 프로토콜에 대한 명세기반 침입탐지 기법이 이루어져야 할 것으로 판단된다.

참 고 문 헌

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” IEEE Transactions on Wireless Communications, vol:1, Issue:4, pp.660-670, Oct. 2002

[2] L. Eschenauer and V.D. Gligor, ″A key management scheme for distributed sensor networks,″ In Proceeding of the 9th ACM conference on Computer and Communications Security. pp.41-47, Nov. 2002

[3] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro. ″SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks″. Fifth IEEE International Symposium on Network Computing and Applications, pp.145-154, July 2006.

[4] P. Banerjee, D. Jacobson, and S. N. Lahiri. ″Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks″. IEEE Proceedings of the 6th IEEE International Symposium on Network Computing and Applications, pp.145-152, July 2007.

[5] D. Wagner, ″Resilient Aggregation Sensor Networks″, ACM SASN ’04, Washington DC, 2004, pp. 78-87

[6] Y. Yang et al., ″SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks″, ACM Mobihoc ’06, Florence, Italy 2006, pp 356-367

[7] L. Buttyan, P. Schaffer, and I. Vajda, ″RANBAR: RANSAC-Based Resilient Aggregation in Sensor Networks″, ACMSAAN ’06, Alexandria, VA, 2006, pp. 83-90

[8] Y. Zhang and W. Lee, ″Intrusion Detection Techniques for Mogile Ad Hoc Networks″, ACM WINET Journal, 2003.

이 윤 호 (Yunho Lee) 정회원

1999년 2월 육군사관학교 전자공학과 학사

2005년 2월 서울대학교 컴퓨터공학과 석사

2009년 1월~현재 국방대학교 국방정보체계 박사과정

<관심분야> 무선통신보안, 키 관리, 침입탐지

강 정 호 (Jungho Kang) 정회원

2000년 2월 육군사관학교 전자공학과 학사

2006년 2월 서울대학교 계산과학 석사

2010년 1월~현재 아주대학교 NCW학과 박사과정

<관심분야> RFID, 네트워크 보안, 클라우드 컴퓨팅

이 수 진 (Soojin Lee) 정회원

1992년 2월 육군사관학교 전산학과 학사

1996년 2월 연세대학교 컴퓨터과학과 석사

2006년 2월 한국과학기술원 전산학과 박사

2006년 3월~현재 국방대학교 국방정보체계학과 교수

<관심분야> 침입탐지, 무선통신보안, 키 관리, 보안정책