지능정보연구 제16권 제1호 2010년 3월(pp.45~56)

무선 센서 네트워크에서 다중 공격 방어를 위한 보안 라우팅 기법

문수영
성균관대학교 정보통신공학부
(moonmous@ece.skku.ac.kr)

조대호
성균관대학교 정보통신공학부
(taecho@ece.skku.ac.kr)

센서 네트워크는 이벤트 감지와 통신 기능이 있는 다수의 센서 노드들과 하나 이상의 싱크 노드들로 이루어진 시스템이다. 센서 네트워크는 배치된 지역에 있는 사물의 인식 정보와 주변의 환경 정보를 수집하여 사용자에게 제공한다. 센서 노드의 자원 제약과 무선통신 사용, 기반 시설의 부재로 인해 센서 네트워크는 여러 보안 위협에 취약하다. 센서 네트워크 보안과 관련한 대부분의 기존 연구는 한 가지 공격을 탐지하고 방어하는 것을 목표로 진행되어왔다. 그러나 실제 센서 네트워크에서는 언제 어떠한 공격이 발생할 지 미리 예측할 수 없으며 동시에 여러 가지 공격이 함께 발생할 가능성도 존재한다. 본 논문에서는 센서 네트워크에서 발생 가능한 공격인 허위 보고서 공격과 웜홀 공격을 방어할 수 있는 보안 라우팅 기법을 제안한다. 제안 기법은 기존 보안 기법을 개선 및 결합함으로써 실험 결과 기존 기법보다 높은 공격 검출 성능을 보인다.

논문접수일 : 2009년 12월 14일 논문수정일 : 2010년 01월 10일 게재확정일 : 2010년 01월 30일 교신저자 : 조대호

1. 서론

센서 네트워크(sensor network)는 이벤트 감지와 연산 기능, 그리고 통신 기능이 있는 센서 노드(sensor node)들과 하나 이상의 싱크 노드들로 구성된 시스템이다(Akyildiz et al., 2002; Al-Karaki and Kamal, 2004). 센서 네트워크는 주변 환경 정보를 실시간으로 감지하여 사용자에게 제공함으로써 효과적인 대응을 가능하게 하는 기술이다. 또한 사물의 인식 정보를 제공하는 무선 식별 기술(Radio Frequency Identification : RFID)과 함께 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network : USN)를 구성한다. 센서 노드는 부착된 센서의 종류에 따라 주변의 환경 정보(빛, 온도, 습도, 움직임 등)를 감지한 후 전기적 신호로 변화하여 메시지의 형태로 싱크 노드(sink node)에게 전달한다. 일반적으로 센서 노드들은 무선 통신을 사용하고 전송 범위가 제한되어 있으므로 싱크 노드에게 전달되는 메시지는 중간에 여러 노드들을 거치게 된다. 싱크 노드는 센서 노드들로부터 수집한 정보를 가공하여 사용자에게 제공한다.

센서 네트워크는 센서 노드들의 에너지를 포함한 자원 측면에서의 제약과 무선통신 사용 및 기반 시설 부재 등의 특징으로 인해 여러 보안 위협

* 이 논문 또는 저서는 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2008-313-D00827).

에 취약하다(Karlof and Wagner, 2003; Djenouri et al., 2005). 센서 네트워크에서 발생 가능한 공격과 대응 방안에 대해 현재까지 많은 연구가 이루어져 왔다. 대부분의 기존 연구에서는 공격의 종류를 한 가지로 고정하여 이를 탐지하고 방어하는 것을 목표로 한다. 하지만 실제 센서 네트워크에서는 언제 어떤 공격이 발생할 지 미리 예측할 수가 없으며 동시에 두 개 이상의 공격이 복합적으로 발생할 가능성도 존재한다. 제안 기법에서는 이러한 문제점을 해결하기 위해 센서 네트워크에서 발생할 수 있는 공격인 허위 보고서 공격과 웜홀 공격을 방어할 수 있는 보안 라우팅 기법을 제안한다. 제안 기법은 기존 보안 기법을 결합 및 개선함으로써 구성되었으며 위의 두 가지 공격을 모두 탐지하고 방어할 수 있다. 시뮬레이션을 통해 제안 기법이 기존 보안 기법에 비해 공격 탐지 성능이 더 높음을 확인하였다.

본 논문의 구성은 다음과 같다. 먼저 제 2장에서는 제안 기법에서 방어를 목적으로 하는 웜홀 공격과 허위 보고서 공격의 특징을 살펴 보고 각각의 공격에 대한 기존 보안 기법의 동작 과정과 특징에 대해 설명한다. 제 3장에서는 제안 기법의 동기와 가정 사항, 공격 모델 및 동작 과정을 기술한다. 제 4장에서는 제안 기법과 기존 기법의 공격 검출 성능을 비교한 결과를 보이고 제 5장에서는 결론과 추후 연구 방향을 제시한다.

2. 배경 이론

본 장에서는 허위 보고서와 웜홀 공격, 기존 보안 기법에 대해 설명하고 단일 공격과 다중 공격 환경의 차이점에 대해 설명한다.

2.1 허위 보고서 공격

허위 보고서 공격에서 공격자는 센서 노드 중 일부를 탈취하여 해당 노드들에 저장된 보안 관련 정보 및 제어권을 획득한다. 공격자에 의해 획득된 노드를 훼손 노드(compromised node)라 한다. 공격자는 훼손 노드를 이용해 존재하지 않는 이벤트 정보를 담은 허위 보고서를 생성하여 네트워크 내에 주입한다. 이러한 허위 보고서는 싱크 노드까지 전달되는 과정에서 중간 노드들의 에너지를 고갈시키고 싱크 노드를 기만하여 사용자를 혼란에 빠트리게 한다(Ye et al., 2005). 센서 네트워크에 노드 간의 메시지 인증 기능을 제공하는 프로토콜이 사용되는 경우, 훼손된 노드는 자신이 가진 키와 전송 범위 안의 다른 훼손 노드가 가진 키를 이용하여 인증 정보를 생성하고 보고서에 덧붙임으로써 메시지 인증 기능을 무력화시킨다.

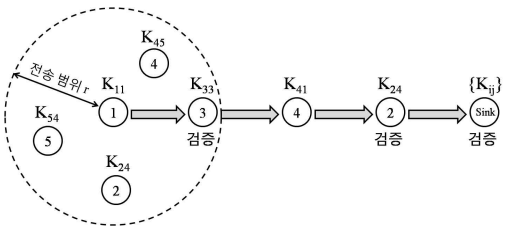
2.2 통계적 여과 기법

이러한 허위 보고서 공격을 방어하기 위해 많은 보안 기법들이(Choi and Cho, 2009, Lee and Cho, 2007; Li and Wu, 2006; Nghiem and Cho, 2009; Ye et al., 2005; Yu and Guan, 2006; Zhu, 2007) 제안되었다. 그 중 통계적 여과 기법(Ye et al., 2005)은 허위 보고서 공격을 방어하기 위해 Fan Ye 등에 의해 제안된 기법이다. SEF에서는 싱크 노드가 전역 키 집합(Global key pool)을 관리한다. 전역 키 집합은 여러 개의 키 구획(key partition)으로 나뉘며 각각의 노드는 하나의 키 구획에 속한 키 중 일부를 할당 받는다. 대상 지역에서 이벤트 발생 시 이를 감지한 노드 중 하나가 대표 노드로 선출된다. 대표 노드는 타 감지 노드들로부터 해당 이벤트 정보에 대한 메시지 인증 코드(message au-

thentication code; 이하 MAC)들을 수집한다. MAC은 각각의 노드가 가진 인증 키 중 하나를 사용해서 해당 이벤트 정보를 암호화 한 결과값이다. 이 때 대표 노드는 t개의 서로 다른 키 구획에 속한 키로 만들어진 MAC을 선택하여 이벤트 보고서를 구성한다. 보고서 전달 과정에서 중간 노드들은 자신이 가진 키로 생성된 MAC이 보고서 내에 존재하면 직접 해당 MAC을 계산하여 보고서 내 MAC과 같은 지를 검사하고 두 MAC이 다른 경우에는 허위 보고서로 간주하여 제거한다. <그림 1>은 SEF의 동작 과정을 보여 준다.

<그림 1>에서 각각의 원과 그 안의 숫자는 센서 노드 와 해당 키 구획 정보를 나타낸다. K_{ij}는 해당 노드에 할당된 키가 i번째 키 구획의 j번째 키라는 것을 의미한다. 위 예에서는 K_{11} 키를 가진 노드가 대표 노드가 되어 주변 노드들로부터 MAC을 수집한다. 수집된 MAC은 이벤트 보고서에 포함되어 다음 노드로 전달된다. 중간 노드들은 자신이 가진 키로 생성된 MAC이 보고서 내에 존재하면 해당 MAC을 검증하고 두 값이 일치하는 경우에만 다음 노드로 전달한다. 싱크 노드는 모든 키를 다 갖고 있기 때문에 보고서 내 모든 MAC을 검증할 수 있다.

SEF는 서로 다른 키 구획에 해당하는 노드들이 서로 협력하여 보고서를 인증하도록 함으로써 훼손 노드에 의한 허위 보고서 공격을 방어할 수 있다. 또한 네트워크의 규모가 커질수록 이벤트 보고서가 거치는 중간 노드의 수가 많아지기 때문에 허위 보고서가 검출될 확률도 높아지는 장점이 있다. SEF에서 각 중간 노드는 확률적으로 이벤트 보고서를 검증하기 때문에 보고서 전달 경로는 허위 보고서 검출 성능에 영향을 미치게 된다.



<그림 1> SEF 동작 과정

2.3 웜홀 공격

웜홀 공격(wormhole attack)은 센서 네트워크의 라우팅 경로 내에 공격 노드를 포함시키는 공격으로 선택적 전달이나 메시지 변조와 같은 추가적 공격을 가능하게 한다. 웜홀 공격은 일반적으로 두 개의 공격 노드가 쌍을 이루어 동작한다. 하나의 공격 노드가 주변의 정상 메시지를 도청하여 터널을 통해 맞은 편 공격 노드로 전달하면 이를 수신한 공격 노드는 해당 메시지를 자신의 주변 지역 노드들에게 브로드캐스팅(broadcasting) 한다. 웜홀을 통과한 메시지를 수신한 정상 노드들은 해당 메시지가 자신의 이웃 노드로부터 온 것으로 오인하게 된다. 터널은 공격 노드만이 사용할 수 있는 연결로서 논리적 터널, 고주파 통신 혹은 유선 연결 등의 방법으로 구현된다(전효진 등, 2006). 센서 네트워크의 라우팅 경로 설정 단계에서는 일반적으로 싱크 노드에서 초기화된 라우팅 메시지가 브로드캐스팅 방식으로 전달되며 이를 수신한 노드는 싱크 노드를 부모 노드로 지정하고 다시 브로드캐스팅 한다. 각 노드는 자신이 최초로 수신한 라우팅 메시지의 송신 노드를 자신의 부모 노드로 지정하고 브로드캐스팅 하는 과정을 반복한다. 라우팅 메시지가 웜홀을 통과하는 경우 정상 노드들을 거쳐 전달되는 것보다 대상 지역에 더 빨리 도착하게 되므로 라우팅 경로 내에 공격 노드가 포함되는 결과를 가져 온다. 웜홀 공격은 센

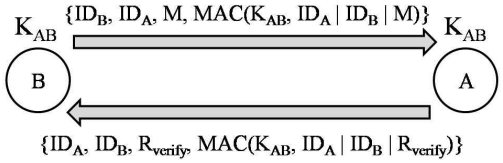
서 네트워크의 라우팅 경로를 왜곡시켜 터널로 연결된 두 지점 사이를 단절시키는 효과가 있으며 공격자의 의도에 따라 웜홀을 통과하는 메시지에 대해 선택적 전달이나 메시지 변조 등의 공격이 가능하다.

2.4 웜홀 방어 보안 라우팅 프로토콜

이러한 웜홀 공격을 방어하기 위해 보안 기법들(전효진 등, 2006; Hu et al., 2006; Madria and Yin, 2009; Yun et al., 2007)이 제안되었다. 이 중 웜홀 방어 보안 라우팅 프로토콜(Secure routing protocol against wormhole attack; 이하 SeRWA)(Madria and Yin, 2009)은 웜홀 탐지 및 방어를 위해 Madria 등에 의해 제안된 기법이다. SeRWA에서는 이웃 노드 탐색 단계와 데이터 전달 단계에서 웜홀 검출을 수행한다. 이웃 노드 탐색 단계에서는 통신 가능 범위 내에 위치한 노드 사이에 Hello, Response 메시지를 사용하여 이웃 노드 관계를 설정한다. 임의의 두 이웃 노드 사이의 거리가 매우 가깝다고 추정되는 경우 두 노드는 웜홀로 연결되었을 가능성이 있다고 판단한다. 두 이웃 노드 사이의 거리는 두 노드가 공유하지 않는 이웃 노드의 수로 예측할 수 있다. 따라서 모든 노드는 자신의 이웃 노드 목록을 모든 이웃 노드와 교환한다. 두 이웃 노드가 공유하지 않는 이웃 노드의 개수가 임계값(threshold value)보다 작은 경우 두 노드는 웜홀로 연결되었을 가능성이 있다고 판단하여 이웃 노드 목록 재설정 과정을 수행하게 된다. 이웃 노드 목록 재설정 단계에서는 웜홀 연결이 의심되는 두 노드 뿐만 아니라 두 노드의 모든 이웃 노드들 또한 웜홀로 연결되었을 가능성이 있는 모든 이웃 노드를 자신의 이웃 노드 목록에서 제거한다. 이웃 노드 탐색 단계 이후 모든 노드는 자신의 이웃 노드와 공유하는 인증 키를 생성한다. 데이터 전달 단계에서는 센서 노드들이 사용하는 채널이 신뢰할 수 있다는 가정 하에 웜홀을 검출한다. 이웃 노드 단계에서 검출되지 않은 웜홀에서 메시지 제거 혹은 변조 공격이 발생한 경우 메시지 송신 측 혹은 수신 측 노드는 이를 감지하고 이웃 노드 재설정 단계를 수행한다. <그림 2>는 SeRWA의 메시지 전달 과정을 보여준다.

<그림 2>에서 B와 A는 이웃 노드이고 IDB, IDA는 B와 A의 ID를 의미하며 M은 B에서 A로 전달되는 메시지 내용이다. B와 A는 공유키 KAB를 각자 갖고 있으며 이 키를 이용해 MAC을 생성한다. B가 A에게 메시지를 전달하면 A는 자신이 가진 공유키로 MAC을 생성하여 메시지 내용을 검증하고 그 결과를 Rverify 값에 저장하여 ACK 메시지로 반환한다. ACK 메시지 역시 공유키 KAB로 인증된다. B와 A가 웜홀로 연결되어 있는 경우 웜홀에서 메시지를 제거하면 A로부터 ACK 메시지가 오지 않기 때문에 B에서 웜홀이 검출된다. 또한 메시지 내용이 변경되는 경우 A 또는 A와 B 모두에서 웜홀이 검출된다.

SeRWA는 웜홀을 라우팅 경로 설정 단계 이전과 실제 데이터 전달 과정에서 효과적으로 검출하고 대응할 수 있다. 그러나 이웃 노드 탐색 단계에서 검출되지 않는 웜홀이 존재할 수 있고 이러한 웜홀은 메시지 제거 혹은 변경이 발생하지 않는 한 검출되지 않는다.



<그림 2> SeRWA 메시지 전달 과정

2.5 다중 공격 환경

다중 공격 환경은 둘 이상의 공격이 동시에 발생하는 환경이다. 다중 공격 환경에서는 기존 보안 기법의 성능이 단일 공격 환경과 비교하여 향상 또는 저하되는 현상이 나타나는데 그 이유는 다음과 같다. 1) 서로 다른 공격 간의 간섭이 존재한다. 동시에 발생하는 둘 이상의 공격은 서로 영향을 미쳐 새로운 형태의 공격을 만들어 낸다. 이러한 새로운 형태의 공격은 기존 보안 기법에서 공격 검출 및 방어를 위해 사용한 가정사항을 무효화할 수 있다. 2) 서로 다른 보안 기법 간의 간섭이 존재한다. 다중 공격을 방어하기 위해 기존 보안 기법을 여러 개 사용하는 경우 개별 보안 기법 관점에서 사용할 수 있는 데이터의 양이 늘어나게 되어 공격에 대한 검출 및 방어 효율을 향상시킬 수 있다. 한편 하나의 보안 기법의 동작이 메시지 전달 경로를 변경시키거나 다른 보안 기법에서 사용하는 데이터를 변경시켜 단일 공격 환경과 비교하여 보안 기법의 성능이 저하될 가능성도 존재한다.

허위 보고서 공격과 웜홀 공격이 동시에 발생하는 경우, 보고서 전달 경로가 웜홀에 의해 단축되기 때문에 허위 보고서 검출 성능이 저하된다. 또한 또한 전달 경로 내의 훼손된 노드는 허위 보고서 공격과 웜홀 공격 검출을 하지 않기 때문에 웜홀 공격의 검출 성능 또한 저하된다.

이러한 다중 공격 환경에서 공격을 검출하고 방어하기 위해서는 서로 다른 보안 기법 간의 간섭 현상을 분석하고 늘어난 가용 데이터를 효율적으로 사용하는 것이 필요하며 이를 위해 기존 보안 기법을 개선하거나 새로운 보안 기법을 제안하는 것이 필요하다.

3. 제안 기법

본 장에서는 제안 기법에서 가정한 사항들과 공격 모델, 개요, 제안 기법의 동작 과정에 대해 설명한다.

3.1 가정 사항

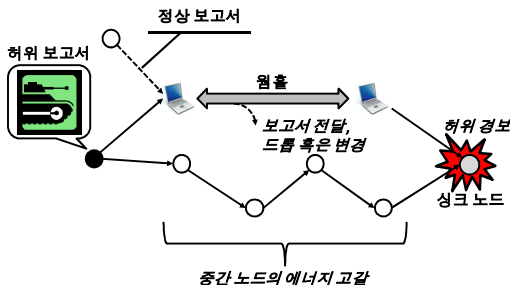
본 논문에서 가정하는 사항들로는 다음과 같은 것이 있다. 각각의 센서 노드는 자신의 위치 정보를 알고 있다. 센서 노드들은 제한된 전송 범위를 가지며 양방향 통신을 사용한다. 공격자는 센서 네트워크 내 임의의 노드를 획득하여 허위 보고서 공격에 사용할 수 있다. 또한 충분한 에너지를 가지며 원거리 고주파 통신이 가능한 장비를 갖는다. 싱크 노드는 노드 포획 등의 공격으로부터 안전하다.

3.2 공격 모델

제안 기법에서 가정하는 공격 모델은 다음과 같다. 공격 노드에는 내부 노드와 외부 노드의 두 종류가 존재한다. 내부 노드는 공격자에 의해 훼손된 센서 노드를 의미하며 외부 노드는 공격자가 소유한 별도의 장비로서 충분한 에너지 자원을 가지며 먼 거리에서 고주파 통신을 할 수 있다. 내부 노드는 공격자에 의해 재프로그램 되어 허위 보고서 공격에 사용되고 외부 노드는 두 개씩 쌍을 이루어 웜홀 공격에 이용된다. 웜홀의 한 쪽 끝에 위치한 외부 노드에 의해 도청된 정상 메시지는 터널을 통해 맞은 편으로 전달되며 이를 수신한 외부 노드는 해당 메시지를 주변에 브로드캐스팅 한다. <그림 3>은 이러한 공격 모델을 나타낸다.

3.3 제안 기법 개요

제안 기법은 크게 4단계의 순서로 동작한다. 노드 배포 전 단계에서는 SEF에서와 동일하게 인증키 및 ID 할당이 이뤄진다. 이웃 노드 탐색 단계에



<그림 3> 공격 모델

서는 이웃 노드들 간 Hello, Response 메시지를 교환함으로써 초기 이웃 노드 관계를 설정한다. 또한 SeRWA에서와 같이 초기 웜홀 검출을 수행한다. 경로 설정 단계에서는 싱크 노드에서 초기화된 라우팅 메시지가 전체 네트워크에 브로드캐스트 되며 이에 따라 라우팅 경로가 형성된다. 데이터 전달 단계에서는 센서 노드들이 이벤트를 감지하여 이벤트 보고서를 생성하고 이를 싱크 노드에게 전달한다. 또한 보고서 전달 과정에서 중간 노드들에 의해 허위 보고서 및 웜홀 공격이 검출된다. 제안 기법은 SEF와 SeRWA를 개선하여 단일 공격과 다중 공격의 검출 및 방어 성능 향상을 목적으로 한다.

3.4 동작 과정

제안 기법의 동작 과정은 다음과 같다. 노드 배포 전 단계는 SEF에서와 마찬가지로 메시지 인증을 위해 노드들에게 전역 키 집합에서 일부 키를 할당한다. 노드의 ID 또한 이 단계에서 결정된다.

이웃 노드 탐색 단계에서는 모든 노드들이 Hello 메시지를 방송하고 이웃 노드로부터 수신한 Hello 메시지에 대해 Response 메시지로 응답한다. Hello 메시지에는 송신 노드의 ID가 포함되어 있으며 Response 메시지에는 송신 노드와 수신 노드의 ID가 포함되어 있다. Hello 메시지를 수신한 노드는 송신 노드의 ID를 이웃 노드 목록에 추가하고 Response 메시지를 생성하여 송신 노드에게 보낸다. Response 메시지를 수신한 노드는 메시지에 포함된 수신 노드의 ID가 자신이면 송신 노드의 ID를 이웃 노드 목록에 추가한다.

경로 탐색 단계에서는 싱크 노드에 의해 초기화된 라우팅 메시지가 전체 네트워크에 전달된다. 기존의 일반적인 라우팅 기법에서와 달리, 제안 기법에서는 개별 노드가 라우팅 메시지 수신 시 부모 노드를 하나만 지정하는 것이 아니라 부모 노드로 사용 가능한 후보 부모 노드들의 목록을 관리하고 이벤트 보고서 전달 시 보안과 에너지 효율성을 고려하여 부모 노드를 선택한다. 라우팅 메시지에는 송신 노드의 ID, 위치, 키 구획 정보가 포함되어 있다. 라우팅 메시지를 수신한 노드는 송신 노드의 위치 정보를 기준으로 송신 노드가 자신보다 싱크 노드에 가까운 경우 해당 노드의 ID, 싱크 노드까지의 거리, 키 구획 정보를 후보 부모 노드 목록에 저장한다. <그림 4>는 라우팅 메시지 형식을 나타낸다.

송신 노드 ID	송신 노드 위치	송신 노드의 키 구획 정보	…

<그림 4> 라우팅 메시지 형식

데이터 전달 단계는 실제 이벤트 발생 시 해당 이벤트에 대한 보고서 생성과 전달, 그리고 허위 보고서 및 웜홀 검출이 이루어지는 단계이다. 이벤트 발생 시 이를 감지한 노드들은 SEF에서와 같이 대표 노드를 선출하고 대표 노드는 다른 감지 노드들의 MAC을 모아 이벤트 보고서를 구성한다. 추가적으로, 제안 기법에서는 웜홀 공격 검출을 위해 이벤트 보고서 내에 MAC 검증 횟수를 추가하여 중간 노드에서 갱신하도록 한다. <그림 5>

송신 노드 ID	이벤트 정보	{(키 인덱스, MAC)}	MAC 검증 횟수

<그림 5> 이벤트 보고서 형식

는 이벤트 보고서의 형식을 보여 준다.

이벤트 메시지 내에는 송신 노드의 ID, 이벤트 관련 정보, t개의 (키 인덱스, MAC) 쌍의 집합, 중간 노드에 의한 MAC이 검증된 횟수가 포함된다.

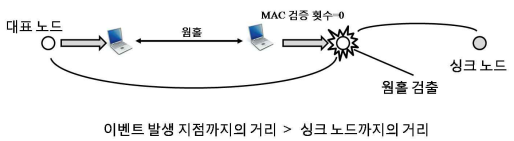
생성된 이벤트 보고서는 대표 노드에 의해 싱크 노드로 전달된다. 보고서 전달 과정에서 중간 노드들은 아래의 순서에 따라 허위 보고서 및 웜홀 검출을 수행한다.

수신된 이벤트 보고서의 송신 노드의 ID가 이웃 노드 목록에 있는지 확인하고 그렇지 않다면 제거한다.

이벤트 발생 지점까지의 거리를 고려하여 예상되는 MAC 검증 횟수를 계산한다. 이벤트 보고서 내 MAC 검증 횟수가 예상되는 검증 횟수보다 적고, 싱크 노드까지의 거리가 이벤트 발생 지점까지의 거리보다 짧은 경우 웜홀이 검출되며 이 때 송신 노드를 이웃 노드 목록에서 제거한다.

노드에 저장된 인증 키를 사용하여 보고서 내 MAC을 확률적으로 검증한다. 싱크 노드에 가까운 노드일수록 높은 확률로 MAC을 검증한다. 검증 결과가 허위 보고서로 판명되는 경우 해당 보고서를 제거하고, 그렇지 않다면 다음 노드로 전달한다.

<그림 6>은 중간 노드에서의 웜홀 검출 과정을 나타낸다.



<그림 6> 제안 기법에서의 웜홀 검출

중간 노드에서 다음 전달 노드의 선택은 아래와 같은 방식으로 이루어진다. 먼저 이벤트 보고서를 전달하고자 하는 노드는 자신의 후보 부모 노드 목록에 있는 노드들에 대해 아래의 평가 함수 값을 계산한다.

$$eval(n) = \alpha \cdot \ factor1 + \beta \cdot \ factor2 \qquad (1)$$

위 식에서 n은 후보 부모 노드이며 α, β는 각각의 factor에 대한 가중치에 해당한다. Factor1과 factor2는 각각 이웃 노드 n의 싱크 노드까지의 거리, 그리고 해당 노드가 허위 보고서를 검출할 확률에 해당한다. 이웃 노드의 키 구획 정보를 고려한 전달 노드 결정은(Lee and Cho, 2009; Sun et al., 2009)에서 제안되었으며 본 논문에서는 추가적으로 이벤트 보고서에 따라 해당 보고서 내의 MAC과 같은 키 구획을 갖는 이웃 노드를 다음 전달 노드로 선택한다. 이웃 노드 n이 싱크 노드까지의 거리가 가깝고 전달하려는 이벤트 보고서 내 MAC 중 하나와 같은 키 구획에 속하는 경우 평가 함수의 결과는 높은 값을 갖는다. 송신 노드는 평가 함수의 결과값이 가장 높은 경우에 해당하는 이웃 노드 n이 부모 노드로 선택한다. 모든 중간 노드는 위와 같은 방식으로 다음 전달 노드를 선택하여 이벤트 보고서를 전달한다. 싱크 노드에서는 이벤트 보고서 수신 시 중간 노드와 마찬가지 방법으로 웜홀 및 허위 보고서 공격을 검출하고 대응한다.

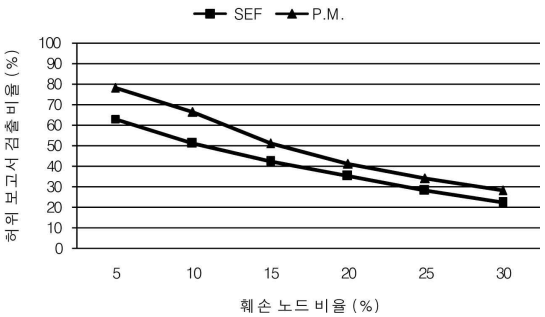
4. 제안 기법 성능 분석

본 장에서는 제안 기법의 성능을 공격 검출 성능 관점에서 기존 기법과 비교 분석한다. 시뮬레이션에 사용된 환경은 다음과 같다. 대상 지역의 크기는 500×500 m^2이며 전체 노드의 수는 600개이

다. 개별 노드는 메시지 송수신 시 한 바이트 당 16.24/12.5μJ을 소비하며 MAC 생성에는 15μJ을 소비한다(Hill et al., 2000; Xbow). 제안 기법의 성능을 공격 검출 성능 관점에서 분석하면 다음과 같다.

제안 기법의 허위 보고서 검출 성능을 SEF와 비교한 결과는 <그림 7>과 같다.

제안 기법은 훼손 노드 비율에 따른 허위 보고서 검출 비율에서 기존 기법인 SEF보다 높은 성

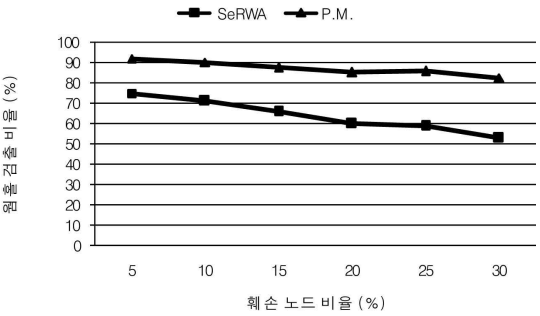


<그림 7> 제안 기법의 허위 보고서 검출 성능

능을 보인다. SEF에서 각 노드가 고정된 부모 노드에게 이벤트 보고서를 전달하는 반면 제안 기법은 이벤트 보고서 내의 MAC과 이웃 노드의 키 구획 정보를 고려하여 허위 보고서 검출 성능이 높은 노드를 부모 노드로 지정한다. 따라서 부모 노드가 변하지 않는 방식에 비해 허위 보고서 검출 확률이 더 우수하다.

웜홀 공격에 대한 방어 관점에서 제안 기법의 성능을 기존 기법인 SeRWA와 비교한 결과는 <그림 8>에 나타나 있다.

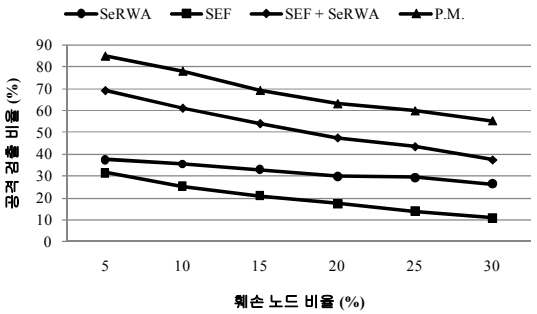
<그림 8>에서 볼 수 있듯이 제안 기법은 훼손 노드의 비율에 따른 웜홀 검출 비율에서 기존 기법인 SeRWA보다 뛰어난 성능을 보인다. 이웃 노드 탐색 단계에서 검출되지 않은 웜홀을 통해 공격이 발생할 수 있다. 이 경우 SeRWA에서는 웜홀 내에서 메시지 드롭 혹은 변조가 일어난 경우에만



<그림 8> 제안 기법의 웜홀 검출 성능

웜홀을 검출 가능하지만 제안 기법에서는 메시지가 웜홀을 단순히 통과만 한 경우에도 해당 웜홀을 검출할 수 있어 보다 높은 웜홀 검출 성능을 보인다.

다중 공격 환경에서의 공격 검출 성능 비교 결과는 <그림 9>에 나타나 있다.



<그림 9> 제안 기법의 다중 공격 검출 성능

<그림 9>에서 SEF+SeRWA는 SEF와 SeRWA가 단순 결합된 보안 기법을 나타낸다. 단순결합기법과 제안 기법과의 차이점은 기존 기법의 개선 여부에 있다. 다중 공격 발생 환경에서 기존 기법과 단순결합기법, 그리고 제안 기법의 공격 검출 성능은 각각의 공격에 대한 검출 성능의 평균으로 정의하였다. 제안 기법은 기존 보안 기법인 SEF와 SeRWA, 그리고 두 기법의 단순결합기법보다 높

은 공격 검출 성능을 보이는 것을 확인할 수 있다.

제안 기법은 추가적인 메시지 전송 없이 허위 보고서 공격과 웜홀 공격, 그리고 두 공격이 동시에 발생하는 다중 공격에 대한 검출 성능을 향상시킬 수 있다. 이벤트 보고서가 전달되는 과정에서 중간 노드에 의해 이벤트 발생 지점까지의 거리와 예상되는 MAC 검증 횟수가 계산되는 것은 이벤트 보고서의 처리 시간을 증가시킬 수 있으나 간단한 산술 연산에 해당하기 때문에 그 영향은 크지 않을 것으로 판단된다. 이벤트 보고서에 포함되는 MAC 검증 횟수의 경우 보고서의 길이를 증가시켜 추가적인 통신 오버헤드를 발생시킬 수 있다. 또한 센서 노드들 간 전달되는 메시지의 길이가 제한될 수 있어 이벤트 보고서의 길이를 줄이기 위한 방법에 대한 연구가 필요하다.

5. 결론

센서 네트워크에서는 발생하는 공격의 종류를 예측할 수 없고 둘 이상의 공격이 동시에 발생할 가능성도 존재한다. 따라서 이러한 다중 공격을 탐지하고 방어할 수 있는 보안 기법이 필요하다. 본 논문에서는 이러한 연구의 출발점으로 허위 보고서와 웜홀 공격을 탐지하고 방어할 수 있는 보안 기법을 제안하였다. 제안 기법은 기존 보안 기법을 결합하고 개선함으로써 단일 공격과 다중 공격 환경에서 기존 보안 기법에 비해 높은 비율로 공격을 검출한다. 앞으로의 연구 목표는 다양한 공격들이 결합된 다중 공격 환경에서 효율적으로 공격을 검출하고 대응할 수 있는 보안 기법의 개발이다.

참고문헌

Akyildiz, I. F., W. Su, Y. Sankarasubramaniam and E. Cayirci, “A Survey on Sensor Networks”, *IEEE Communications Magazine,* Vol.40, No.8(2002), 102~116.

Al Karaki, J. N. and A. E. Kamal, “Routing techniques in wireless sensor networks : a survey”, IEEE Wireless Communication Magazine, Vol.11, No.6(2004), 6~28.

Karlof, C. and D. Wagner, “Secure Routing in Wireless Sensor Networks : Attacks and Countermeasures”, Elsevier, Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, Vol.1, No.2-3(2003), 293~315.

Djenouri, D., L. Khelladi and N. Badache, “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, *IEEE Communications Surveys and Tutorials,* Vol.7, No.4(2005), 2~28.

Ye, F., H. Luo, and S. Lu, “Statistical en route filtering of injected false data in sensor networks”, *IEEE Journal on Selected Areas in Communications,* Vol.23, No.4(2005), 839~850.

Nghiem, P. T. and T. H. Cho, “A fuzzy based interleaved multi-hop authentication scheme in wireless sensor networks”, *Journal of Parallel and Distributed Computing*, Vol.69, No.5(2009), 441~450.

Lee, H. Y. and T. H. Cho, “Fuzzy Based Path Selection Method for Improving the Detection of False Reports in Sensor Networks”, *IEICE Trans. Inf. and Syst.,* Vol.E92 D,No. 8(2009), 1574~1416.

Sun, C. I., H. Y. Lee and T. H. Cho, “A Path Selection Method for Improving the Detection Power of the Statistical Filtering in Sensor Networks”, Journal of Information Science and Engineering, Vol.25, No.4 (2009), 1163~1175.

Lee, H. Y. and T. H. Cho, “Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks”, IEICE Trans. Comm., Vol.E90 B, No.12(2007), 3346~3353.

Zhu, S. “Interleaved hop by hop authentication against false data injection attacks in sensor networks”, ACM Transactions on Sensor Networks(TOSN), Vol.3, No.3(2007), 1~33.

Li, F. and J. Wu, “A Probabilistic Voting based Filtering Scheme in Wireless Sensor Networks”, IWCMC ‘06(2006), 27~32.

Choi, H. M. and T. H. Cho, “Energy Efficient MAC Length Determination Method for Statistical En Route Filtering using Fuzzy Logic”, Lecture Notes in Computer Science, Springer Verlag, LNCS 5754, (2009), 686~695.

전효진, 이건희, 김동규, 서정택, 손기욱, “애드혹 네트워크에서의 이웃노드 정보를 이용한 웜홀 탐지”, 2006년도 한국정보과학회 가을 학술발표 논문집, Vol.33, No.2(C)(2006), 586~591.

Hu, Y. C., A. Perrig, and D. B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, Vol.24, No.2(2006), 370~380.

Madria, S. and J. Yin, “SeRWA : A secure routing protocol against wormhole attacks in sensor networks”, Ad Hoc Networks, Vol.7, No.6(2009), 1051~1063.

Yun, J-H., I-H. Kim, J-H. Lim and S-W. Seo, “WODEM : Wormhole Attack Defense Mechanism in Wireless Sensor Networks”, Lecture Notes in Computer Science (LNCS), Vol.4412(2007), 200~209.

Hill, J., R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, “System Architecture Directions for Networked Sensors”, in Proc. ASPLOS(2000), 93~104.

Xbow sensor networks, http://www.xbow.com.

Abstract

Secure Routing Mechanism to Defend Multiple Attacks in Sensor Networks

Soo Young Moon* · Tae Ho Cho*

Sensor Networks are composed of many sensor nodes, which are capable of sensing, computing, and communicating with each other, and one or more sink node(s). Sensor networks collect information of various objects' identification and surrounding environment. Due to the limited resources of sensor nodes, use of wireless channel, and the lack of infrastructure, sensor networks are vulnerable to security threats. Most research of sensor networks have focused on how to detect and counter one type of attack. However, in real sensor networks, it is impractical to predict the attack to occur. Additionaly, it is possible for multiple attacks to occur in sensor networks. In this paper, we propose the Secure Routing Mechanism to Defend Multiple Attacks in Sensor Networks. The proposed mechanism improves and combines existing security mechanisms, and achieves higher detection rates for single and multiple attacks.

Key Words : Wireless Sensor Networks, Wormhole Attacks, false Report Attacks

* School of Information and Communication Engineering, Sungkyunkwan University

저 자 소 개

문수영
성균관대학교 정보통신공학부 공학사
성균관대학교 전자전기컴퓨터공학과 공학석사
현재 성균관대학교 전자전기컴퓨터공학과 박사과정 재학중
관심분야 무선 센서 네트워크, 라우팅 프로토콜, 침입 탐지, 모델링 시뮬레이션, 인공 지능

조대호
성균관대학교 전자공학과 공학사
University of Alabama 전자공학과 공학석사
University of Arizona 전자 및 컴퓨터공학과 공학박사
현재 성균관대학교 정보통신공학부 교수
관심분야 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템