한국시뮬레이션학회 논문지
Vol. 18, No. 3, pp. 83-90 (2009. 9)

무선 센서 네트워크에서 위조 데이터 주입 공격의 탐지

이해영[1] · 조대호[1†]

Detection of False Data Injection Attacks in Wireless Sensor Networks

Hae Young Lee · Tae Ho Cho

ABSTRACT

Since wireless sensor networks are deployed in open environments, an attacker can physically capture some sensor nodes. Using information of compromised nodes, an attacker can launch false data injection attacks that report non-existent events. False data can cause false alarms and draining the limited energy resources of the forwarding nodes. In order to detect and discard such false data during the forwarding process, various security solutions have been proposed. But since they are prevention-based solutions that involve additional operations, they would be energy-inefficient if the corresponding attacks are not launched. In this paper, we propose a detection method that can detect false data injection attacks without extra overheads. The proposed method is designed based on the signature of false data injection attacks that has been derived through simulation. The proposed method detects the attacks based on the number of reporting nodes, the correctness of the reports, and the variation in the number of the nodes for each event. We show the proposed method can detect a large portion of attacks through simulation.

Key words : Wireless Sensor Networks, Network Security, Security Attack Detection, False Data Injection Attacks

요 약

무선 센서 네트워크는 개방된 환경에 배치된 이후에 방치되므로 공격자는 센서 노드를 물리적으로 포획할 수 있다. 공격자는 포획한 노드의 정보를 사용하여 실재하지 않는 사건을 보고하는 위조 데이터 주입 공격을 수행할 수 있다. 위조 데이터는 허위 경보와 전달 노드들의 제한된 에너지 자원을 고갈시킬 수 있다. 위조 데이터를 전달 과정 중 탐지하여 폐기하기 위한 다양한 보안 기법들이 제안되고 있다. 그러나 이들은 추가적인 작업을 수반하는 예방 기반의 기법들로, 공격이 발생하지 않은 경우에는 에너지 효율적이지 않을 수 있다. 본 논문에서는 추가 비용 없이 위조 데이터 주입 공격을 탐지할 수 있는 기법을 제안한다. 시뮬레이션을 통해 위조 데이터 주입 공격의 서명을 도출하고 이를 기반으로 탐지 기법을 설계한다. 제안 기법은 각 이벤트별로 보고한 노드들의 수, 보고서들의 정확도, 보고 노드 수의 변화량을 기반으로 공격을 탐지한다. 시뮬레이션을 통해 제안 기법이 대부분의 공격을 탐지할 수 있음을 보인다.

주요어 : 무선 센서 네트워크, 네트워크 보안, 보안 공격 탐지, 위조 데이터 주입 공격

1. 서 론

무선 센서 네트워크(wireless sensor network; 이하 WSN)는 다수의 센서 노드들과 소수의 기지 노드(base station; 이하 BS)들로 구성된다[1]. 일반적으로, 센서 노드는 (조도, 온도, 습도, 움직임 등의) 감지, 컴퓨팅, 무선 통신 능력을 가지며 배터리로 구동된다[2]. 노드들은 감시 대상 지역에 무작위로 배치(항공기에 의한 살포 등)되어, 특정 이벤트가 발생하면(적 전차의 출현, 타이머 발생, 사용자의 요청 등) 감지 보고서를 생성하여 BS에게 전달한다. 노드의 통신 범위는 제한적이므로, 대부분의 보고서는 다수의 노드들을 거쳐서 BS에게 전달된다. BS는 보고서들을 모아 사용자에게 전달하거나 사용자의 질의를 해당 노

* 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임. (KRF-2008-313-D00827)
2009년 6월 26일 접수, 2009년 9월 8일 채택
[1] 성균관대학교 정보통신공학부
주 저 자 : 이해영
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

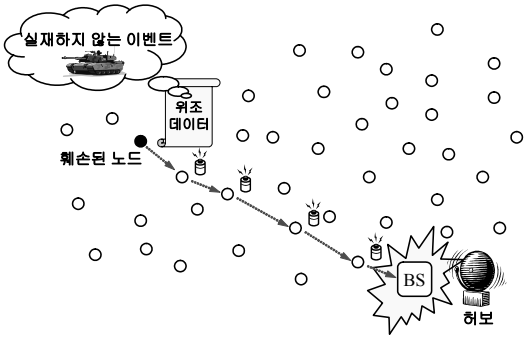

그림 1. 위조 데이터 주입 공격

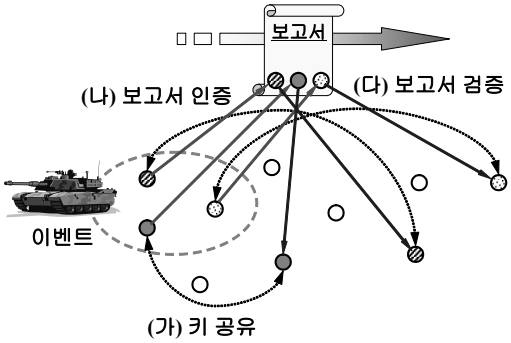

그림 2. 위조 데이터 여과 기법

드에게 전달한다.

WSN에서 노드들은 배치된 이후 별도로 관리되지 않으므로 악의를 가진 공격자는 노드를 손쉽게 물리적으로 파괴, 포획(capture), 훼손(compromise)할 수 있다[3]. 또한 공격자는 그림 1과 같이 훼손한 노드의 암호 키를 사용하여 실재하지 않는 사건을 보고하는 위조 데이터 주입 공격(false data injection attack)을 가할 수 있다[4]. 이러한 위조 데이터는 실세계에서의 대응 노력(병력 투입 등)을 낭비할 수 있는 허보(false alarm)를 유발할 수 있을 뿐만 아니라, 전달 노드들의 제한된 에너지 자원을 고갈시킬 수도 있다[5]. 위조 데이터 주입 공격으로부터 네트워크의 피해를 최소화하기 위해서는 위조 데이터를 전달 과정 중에 탐지하여 폐기할 수 있어야하며 탐지되지 않은 나머지 위조 데이터는 BS에서 식별될 수 있어야한다[6]. 링크 계층의 암호화는 네트워크를 외부 공격자에 의한 위조 데이터 주입 공격으로부터 보호할 수 있으나 훼손된 키를 가진 내부 공격자의 공격으로부터는 보호할 수 없다[7].

노드 훼손 하에서의 위조 데이터를 탐지 및 폐기하기 위한 몇몇 보안 기법들[4-11]이 제안되고 있다. 이들의 특성은 서로 다르지만 기본 아이디어는 유사하다. 각 노드는 특정 노드들과 키를 공유한다(그림 2(가)). 이벤트가 발생하면 감지 보고서를 생성하는데, 여기에는 사전에 정의된 수 t만큼의 노드들이 자신의 키를 사용하여 보고서 내용에 대하여 생성한 메시지 인증 코드(message authentication code; 이하 MAC)들이 포함된다(그림 2(나)). 보고서는 여러 노드들을 거쳐 BS에게 전달되는데, 이 때 각 전달 노드는 가능한 경우 자신의 키를 사용하여 보고서를 검증한다(그림 2(다)). t보다 작은 수의 MAC들을 가졌거나, 검증에 실패한 보고서는 즉시 폐기된다. 이러한 보안 기법은 공격자가 t보다 작은 수의 노드들을 훼손한 경우까지 위조 데이터 주입 공격으로부터 네트워크를 보호할 수 있다. t개의 노드들을 훼손하지 못한 공격자가 위조 데이터 주입 공격을 수행하기 위해서는 t보다 작은 수의 MAC들을 가진 보고서를 생성하거나 최소한 1개의 MAC을 위조해야하는데, 이와 같은 보고서들은 대부분 전달 중에 탐지 및 폐기되기 때문이다. 보안 기법은 이를 통해 네트워크의 에너지 자원을 보존한다. 위조 데이터 주입 공격이 발생한 상황에서는 이러한 보안 기법들을 적용하는 편이 적용하지 않는 편보다 분명 에너지 효율적이다. 그러나 공격이 발생하지 않는 상황에서 보안 기법들은 미적용한 경우보다 많은 에너지를 소비(주로 전달 과정 중 검증으로 인한)하는 문제점을 공통적으로 가진다.

본 논문에서는 이동 물체 추적을 위한 WSN에서 전달 과정 중 추가 에너지를 소비하지 않는 위조 데이터 주입 공격 탐지 기법을 제안한다. 제안 기법은 BS 내에 위치하며, 수집된 보고서들은 버퍼에 일정 시간동안 저장된다. 제안 기법은 수집한 보고서들을 이벤트 단위로 분석하여 공격 여부를 판별한다. 시뮬레이션을 통해 도출된 위조 데이터 주입 공격의 서명(signature)을 기반으로 공격을 판별한다. 시뮬레이션을 통해 제안 기법이 대부분의 공격을 탐지할 수 있음을 보이며, 보고서들이 버퍼에 저장되는 시간을 늘림에 따라 위양성 비율(false positive ratio) 및 위음성 비율(false negative ratio) 비율을 줄일 수 있음을 보인다. 위조 데이터 주입 공격이 탐지된 후에 기존의 보안 기법들을 가동시킨다면 보다 에너지 효율적으로 공격에 대응할 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 위조 데이터 주입 공격의 대응 기법들을 간단히 소개하며, 3장에서는 제안 기법을 자세히 설명한다. 4장에서는 시뮬레이션 결과를 살펴보고, 5장에서는 결론 및 향후 과제를 논한다.

2. 위조 데이터 주입 공격의 대응 기법

본 장에서는 대표적인 위조 데이터 주입 공격에 대한

보안 기법들을 간단히 소개한다.

2.1 통계적 여과 기법

Ye *et al.*이 제안한 통계적 여과 기법(statistical en-route filtering; 이하 SEF)[7]은 노드 훼손 하에서의 위조 데이터 주입 공격 문제를 다룬 최초의 보안 기법이다. SEF는 이후 제안된 보안 기법들의 기초가 되었다. SEF에서 BS는 모든 키들을 전역 키 풀(global key pool)에 두어 관리하며, 노드는 키 풀에서 무작위로 선택된 소수의 키들을 배치 전에 공유한다(그림 3(가)). 이벤트가 발생하면 이를 감지한 각 감지 노드는 자신이 가지고 있는 키들 중 하나의 키를 사용하여 MAC을 생성한다. 대표 노드는 이들 MAC들을 모아 보고서를 생성하여 BS로 전달한다. 보고서가 BS를 향해 전달될 때, 각 전달 노드는 보고서에 포함된 MAC들을 만든 키들 중 하나를 가지고 있다면 보고서를 검증하며, 그렇지 않으면 검증하지 않고 다음 노드에게 넘긴다. SEF에서 보고서는 확률적으로 검증되므로, 위조 데이터는 전달 과정 중 탐지되지 않을 수도 있다. 그렇지만 BS는 모든 키들을 가지고 있으므로 위조 데이터는 BS에서 탐지된다. SEF의 장점으로는 라우팅 프로토콜에 독립적이라는 점과 낮은 검증 비용을 들 수 있다. 그러나 SEF는 전달 중 위조 데이터 탐지 확률이 상대적으로 떨어지며[12], 노드 훼손에 따른 피해를 전역적으로 받는다는 단점도 가진다. 즉, 공격자가 일정 수 이상의 노드들을 훼손한 경우, 전체 네트워크가 위조 데이터 주입 공격에 무력해질 수 있다.

2.2 인터리브드 홉단위 인증 기법

Zhu *et al.*이 제안한 인터리브드 홉단위 인증 기법(interleaved hop-by-hop authentication; 이하 IHA)[4]은 SEF와는 달리 위조 데이터를 결정적으로 탐지하는 보안 기법이다. 두 기법들과는 달리 클러스터 기반의 계층적 라우팅 프로토콜을 적용한 WSN에서 사용할 수 있다. 각 노드는 라우팅 경로 상에서 일정 홉만큼 떨어진 상류(BS 방향) 노드 및 하류(단말 노드 방향) 노드와 키들을 공유한다(그림 3(나)). 이벤트가 발생하면 이를 감지한 클러스터 내의 각 노드는 상위 노드와 공유하는 키를 사용하여 MAC을 생성한다. 클러스터 헤드(cluster head; 이하 CH)는 이들 MAC들을 모아 보고서를 생성하여 BS로 전달한다. 각 전달 노드는 하류 노드와 공유하는 키를 사용하여 보고서의 해당 MAC을 검증한다. 검증에 성공한 경우, 해당 MAC을 제거하고 상류 노드와 공유하는 키를 사용하여 MAC을 생성하여 보고서에 덧붙인다. 마지막으로 다음 노드에게 보고서를 전달한다. IHA에서 위조 데이터는 일정 홉 이내에 반드시 탐지된다. IHA는 빠른 위조 데이터 조기 탐지 능력과 노드 훼손에 의한 피해가 라우팅 경로로 국한되는 장점으로 가진다. 그러나 모든 전달 노드가 검증에 참여하므로 높은 검증 비용을 필요로 하며[12], 라우팅 경로 변화에 따른 비용 역시 매우 크다는 단점을 가진다.

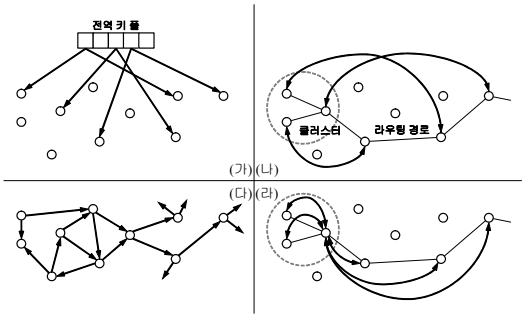

그림 3. 대표적 보안 기법들에서의 키 공유 방식들

2.3 동적 여과 기법

Yu and Guan이 제안한 동적 여과 기법(dynamic en-route filtering; 이하 DEF)[8]는 SEF의 개선 버전이라고 할 수 있다. DEF에서도 SEF와 같이 전역 키 풀에서 임의의 키(DEF에서는 '비밀 키'라고 함)들이 노드에 배치 전에 탑재되는데, 추가적으로 BS와 공유하는 인증 키도 탑재된다. 노드 배치 이후 노드들은 자신의 인증 키를 비밀 키들로 암호화하여 주위 노드들에게 무작위로 배포한다(그림 3(다)). 이를 받은 노드들 중 인증 키를 암호화한 키들 중 하나를 가진 노드는 이를 복호화하여 저장한다. 에너지 절약을 위하여 암호화된 인증 키는 일정 홉까지만 전달된다. 인증 키의 분배가 완료된 이후, 이벤트가 발생하면 이를 감지한 각 감지 노드는 자신의 인증 키를 사용하여 MAC을 생성한다. 대표 노드는 이들 MAC들을 모아 보고서를 생성하여 BS로 전달한 다. 각 전달 노드는 보고서에 포함된 MAC들을 만든 인증 키들 중 하나를 가지고 있다면 보고서를 검증하며, 그렇지 않으면 검증하지 않고 다음 노드에게 넘긴다. DEF에서 역시 보고서는 확률적으로 검증되어 위조 데이터가 전달 과정 중 탐지되지 않을 수도 있다. 그렇지만 인증 키들이 주위 노드들에게 배포됨으로써 SEF보다 위조 데이터를 조기 탐지할 가능성이 높으며, 역시 BS에서 모든 위조 데이터의 식별이 가능하다. DEF도 역시 라우팅 프로토콜에 독립적이며 일정 홉을 지난 이후에는 인증 키들이 배포되지 않아 검증 비

용을 크게 주는 장점을 가진다. 또한, SEF와는 달리 DEF에서 노드 훼손으로 인한 피해는 지역적이다. 그러나 DEF는 전달 중 폐기되지 않는(그러나 BS에서는 식별되는) 위조 데이터를 손쉽게 주입할 수 있는 문제점을 가진다. 이는 인증 키들이 일정 경계 이상으로 배포되지 않는 것에 기인한다.

2.4 키 상속 기반 여과 기법

키 상속 기반 여과 기법(key inheritance-based filtering; 이하 KIF)[9]는 조기 탐지 능력을 극대화한 IHA의 확장 버전이다. KIF에서 위조 데이터는 위조 데이터를 주입한 바로 다음 노드에서 탐지되어 폐기된다. KIF에서 각 노드는 일정 홉 안의 모든 상류 노드들과 키를 공유한다(그림 3(라)). 이벤트가 발생하면, 클러스터의 각 노드는 자신의 키들을 사용하여 MAC들을 생성하고, CH는 이를 수집하여 보고서를 생성한다. 보고서는 다수의 홉들을 지나 BS에 전달되는데, 각 전달 노드는 자신의 키들을 사용하여 MAC들을 생성하고, 보고서에 첨부된 MAC들과 비교한다. 하나를 제외하고 모든 MAC들이 일치하는 경우 보고서는 인증된다. 보고서가 인증되면 노드가 생성한 MAC들을 기존 보고서의 MAC들 위에 덮어쓰고 상류 노드로 전달한다. 인증에 실패한 보고서는 즉각 폐기된다. KIF에서 위조 데이터는 최대 1홉까지 이동할 수 있으며(즉, 결정적이다), 클러스터 기반의 계층적 라우팅 프로토콜을 적용한 WSN에서 동작한다. KIF의 조기 탐지 능력은 위의 보안 기법들보다 뛰어난 것은 장점이나, 이에 따른 막대한 검증 비용은 큰 단점이다[12]. KIF에서 노드 훼손에 따른 피해는 IHA와 동일하게 지역적이다.

3. 위조 데이터 주입 공격 탐지 기법

본 장에서는 제안 기법에 관하여 자세히 설명한다. 먼저 시뮬레이션을 통해 위조 데이터 주입 공격의 특징을 분석하고, 이를 기반으로 공격 탐지 시스템을 제안한다.

3.1 네트워크 모델

제안 기법에서는 WSN의 가장 중요한 응용분야들 중 하나인 이동 물체 추적[13]을 위한 대규모 WSN을 고려한다. 센서 노드들은 높은 밀도로 배치되어 하나의 물체를 다수의 노드들이 감지할 수 있다고 가정한다. 물체를 감지한 각 노드는 감지 보고서를 작성하여 BS로 전달하는데, 보고서에는 노드의 식별자, 물체의 종류, 감지 시각, 물체의 위치, 보고서 내용에 대한 MAC 등이 포함된다. 각 노드는 BS와 유일한 키를 공유하며, 보고서에 포함되는 MAC은 이 키를 사용하여 생성한다. 보고서는 다수의 노드들을 거쳐 BS로 전달되는데, 이 때 에너지를 절약하기 위하여 전달 중에 보고서들이 결합될 수도 있다. 그러나 보고서들에 포함된 MAC들은 버려지지 않는다고 가정한다. 각 노드의 컴퓨팅 및 통신 능력, 에너지 자원은 현세대 노드(MICAz[14] 등)와 유사하다. 노드는 물리적으로 포획될 수 있으나, 비용 문제로 변경 방지(tamper-resistant) 하드웨어에를 적용하지 않는다. 그러므로 공격자는 포획된 노드를 훼손하여 다양한 보안 공격을 가할 수 있다. 그러나 BS는 훼손되지 않는다고 가정한다. BS는 각 노드의 대략적인 위치를 알고 있다. 이동 물체들은 센서 필드 밖에서 필드 안으로 움직임으로써 추적이 시작된다고 가정한다. 즉, 물체가 센서 필드의 경계가 아닌 중간 지역에서 나타나지는 않는다고 가정한다.

3.2 공격자 모델

공격자는 외부 노드들을 사용하거나 네트워크의 노드들을 포획 및 훼손하여 위조 데이터 주입 공격을 네트워크에 가할 수 있다. 발각되지 않고 다수의 노드들을 훼손하는 것은 극히 어려우므로, 다수의 노드들을 훼손할 수는 없다고 가정한다. 공격자는 훼손된 노드들의 정보를 활용하여 훼손된 노드들이 배치되었던 지역이 아닌 네트워크 내의 다른 지역에서 공격을 수행할 수도 있다. 또한, 공격자는 공격의 효과를 극대화하기 위하여 하나의 노드가 다수의 노드들을 표현하는 사이빌(Sybil) 공격[15]을 병행할 수 있다. 그러나 공격자는 훼손하지 않는 노드들의 식별자와 위치는 알 수 없다. 제안 기법에서는 위조 데이터 주입 공격의 탐지만을 대상으로 한다. 위조 데이터 주입 공격 탐지 이후의 조치나 다른 보안 공격의 탐지는 본 논문의 범위를 벗어난다.

3.3 위조 데이터 주입 공격의 서명

위조 데이터 주입 공격의 탐지를 위해서는 먼저 공격의 서명을 분석할 필요가 있다. 위에서 설명된 네트워크 및 공격자 모델에 대하여 시뮬레이션을 수행하여 위조 데이터 주입 공격의 서명을 분석해 보았다. 시뮬레이션을 통해 도출된 공격의 서명은 다음과 같다.

일정 시간 동안 하나의 이동 물체를 보고한 보고서들의 평균 정확도(correctness)가 낮은 경우 위조 데이터 주입 공격일 가능성이 높다. 보고서가 정확한지 여부는 보고서의 MAC 검증 결과 및 노드와 물체와의 거리를 기반으로 결정된다. BS는 하나의 보고서를 받으면, 보고서를

생성한 노드와 공유하는 키를 사용하여 보고서의 MAC을 검증한다. 또한, 노드가 보고한 물체가 노드의 감지 범위 내에 있는지를 확인한다. MAC 검증을 통과하고, 물체가 노드의 감지 범위 내에 있는 경우에만 보고서는 정확하며, 그렇지 않은 경우에는 보고서는 부정확하다. 한 물체에 대하여, 보고서들의 평균 정확도는 정확한 보고서들의 수를 전체 보고서들의 수로 나누어 구한다. 실재 이동 물체를 보고한 정상 보고서들의 경우, 평균 정확도는 100%에 근접한다. 이에 반해 외부 공격자가 위조 데이터 주입 공격을 가한 경우, 위조 MAC들을 붙이므로 평균 정확도는 0%에 근접한다. 또한, 내부 공격자가 사이빌 공격과 함께 위조 데이터 주입 공격을 가한 경우에도 흉내 내려는 노드(표현 노드)들의 키들을 가지고 있지 않으므로 대부분의 보고서들에 위조 MAC들을 붙일 수밖에 없어 평균 정확도가 매우 떨어진다(그림 4(가)). 추가적으로, 실재하지 않는 물체가 이동하는 것처럼 위장하기 위하여 보고서에서 위치를 조작하는 경우에도 평균 정확도가 떨어진다. 그러므로 보고서들의 늦은 평균 정확도는 위조 데이터 주입 공격의 서명이라 할 수 있다. 그러나 내부 공격자가 훼손한 노드들의 키들만을 사용하여 위조 데이터 주입 공격을 가한 경우에는 평균 정확도는 정상 보고서들의 정확도와 유사할 수 있다.

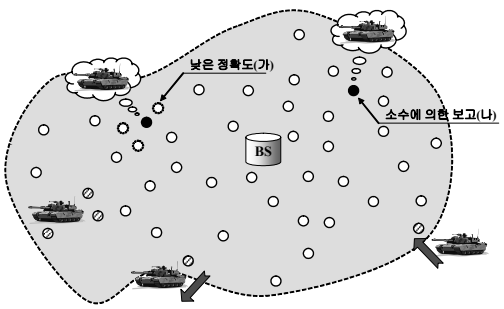

그림 4. 위조 데이터 주입 공격의 대표적인 서명

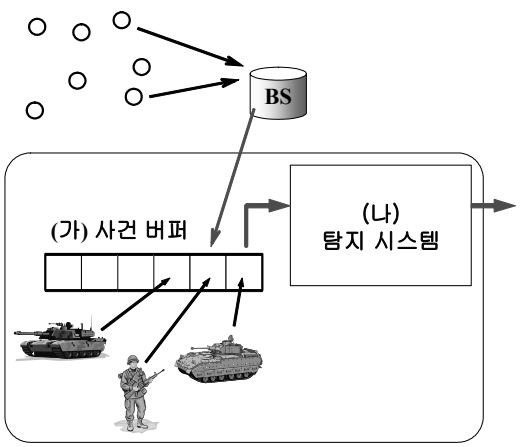

그림 5. 제안 공격 탐지 기법의 구조

일정 시간 동안 하나의 물체를 보고한 노드들의 수가 작은 경우 위조 데이터 주입 공격일 가능성이 높다. 공격자가 발각되지 않고 다수의 노드들을 훼손하는 것은 매우 어렵다. 그러므로 공격자는 소수의 훼손된 노드들만을 사용하여 위조 데이터 주입 공격을 가할 수밖에 없다(그림 4(나)). 이에 반해 실재 이동 물체는 네트워크의 밀도가 매우 높으므로 다수의 노드들에 의해 감지된다. 또한, 물체가 실제 센서 필드 위에서 이동함에 따라 이를 보고하는 노드들의 수 역시 증가한다. 즉, 실재하는 이동 물체의 경우, 이를 보고하는 노드들의 수가 일반적으로 일정 수 이상이 된다. 그러므로 이동 물체를 보고하는 노드들의 수가 작은 것은 위조 데이터 주입 공격의 서명이라 할 수 있다. 그러나 사이빌 공격과 위조 데이터 주입 공격을 조합한 경우에는 이동 물체를 보고하는 노드들의 수가 실재 물체를 보고하는 노드들의 수와 유사할 수 있다. 또한, 실제 이동 물체가 센서 필드로 진입하는 경우(즉, 추적이 시작되는 시점)와 이동 물체가 센서 필드를 탈출하는 경우(즉, 추적이 종료되는 시점)에는 정상임에도 불구하고 이를 보고하는 노드들의 수가 작을 수 있다.

이 외에도 다양한 위조 데이터 주입 공격의 서명이 존재한다. 예를 들어, 센서 필드의 경계가 아닌, 필드 내부 지역에서 이동 물체가 출현한 경우 위조 데이터 주입 공격일 가능성이 높다. 또한, 거의 움직이지 않는 물체들은 위조 데이터 주입 공격일 가능성이 높다. 그러나 대부분의 현상들은 앞서 도출된 두 서명을 동반한다. 공격을 통해 센서 필드 내부에서 물체가 출현한 것처럼 만든 경우, 이를 보고한 노드들의 수가 작거나, 수는 많지만 정확도가 떨어진다. 거의 움직이지 않는 물체의 경우 이를 보고한 노드들의 수가 작을 수밖에 없다.

3.4 위조 데이터 주입 공격 탐지 기법의 구조

그림 5는 제안 위조 데이터 주입 공격 탐지 기법의 구조를 나타낸 그림이다. 제안 기법은 BS 또는 사용자 시스템 내에 위치하며, 사건 버퍼와 탐지 시스템으로 구성된다. BS에서 수집된 감지 보고서들의 사본은 제안 기법의 버퍼에 사건별로 분류되어 사건 정의된 단위 시간 T동안 저장된다(가). 탐지 시스템은 사건 버퍼에 저장된 보고서들을 각 사건 별로 분석하여 공격 여부를 판별한다(나). 공격으로 판별된 사건의 경우, 사용자에게 해당 사건을

보고한 노드들과 사건의 위치를 알린다. 사용자는 해당 사건을 검토한 이후, 적절한 보안 기법을 활성화하거나 대응 인력을 투입하는 등의 조치를 취한다.

3.5 공격 여부의 판별

제안 기법에 포함된 탐지 시스템은 감지 보고서들을 분석하여 위조 데이터 주입 공격 여부를 판별한다. 먼저 시스템은 사건 버퍼에 저장된 각 사건에 대하여, 해당 보고서들을 분석하여 T 동안 사건을 보고한 보고서들의 평균 정확도 C, T 동안 사건을 보고한 노드들의 수 N, T 동안 N의 변화량 V를 구한다. V가 음의 값인 경우에는 사라져가는 사건(물체가 센서 필드 밖으로 나가거나 파괴됨)임을, 양의 값인 경우에는 새로이 나타나는 사건(물체가 센서 필드 안으로 진입함)임을 의미한다.

먼저 C가 사전에 정의된 임계 값(threshold value) C_{min} 미만인 경우(즉, $C < C_{min}$), 탐지 시스템은 해당 사건을 공격으로 판별한다. 해당 조건은 보고서들에 첨부된 MAC들 중 대부분이 틀리거나, 사건의 위치가 이를 보고한 대부분의 노드들의 탐지 범위 밖에 있음을 의미하고, 이는 외부 공격자에 의한 위조 데이터 주입 공격이나, (내·외부 공격자에 의한) 사이빌 공격이 병행된 위조 데이터 주입 공격의 전형적인 서명이기 때문이다.

C가 C_{min} 이상이지만, N이 사전에 정의된 임계 값 N_{min} 미만이고, V가 사전 정의된 임계 값 V_{min}이상인 경우(즉, $C \geq C_{min} \wedge N < N_{min} \wedge V \geq V_{min}$), 탐지 시스템은 해당 사건을 공격으로 판별한다. $N < N_{min}$은 해당 사건이 작은 수의 노드들에 보고되었음을 의미하고, 이는 제한된 수의 훼손된 노드들을 사용한(내부 공격자에 의한) 위조 데이터 주입 공격의 전형적인 서명이다. 이 공격에서는 훼손된 노드들 사용하므로 일반적으로 $C \geq C_{min}$이다.

그러나 실재 물체가 파괴되거나 센서 필드 밖으로 이동하는 등 사라져가는 경우에도 비슷한 현상이 나타날 수 있다. 즉, 이러한 사건들의 N은 실재 사건임에도 불구하고 임계 N_{min}을 넘기지 못할 수 있다(물론, 실재 사건이므로 일반적으로 $C \geq C_{min}$이다). 그러므로 제안 기법에서는 사건을 보고하는 노드들 수의 변화량(V)을 함께 고려한다. 일반적으로 사라져가는 사건의 경우에는 V는 음수(즉, 보고 노드들의 수가 줄어듦)이지만, 위조 데이터 주입 공격에서 V는 양수(즉, 공격 시작으로 보고 노드들의 수가 늘어남)이기 때문이다.

또한 실재하는 물체가 새로이 나타나는 경우에도 보고 노드들의 수가 임계 값 미만일 수 있으나, 이는 큰 값의 T를 적용함으로써 제외시킬 수 있다. 물체가 센서 필드에 진입할수록 이를 보고하는 노드들의 수가 늘어나기 때문이다. 또한, 이 경우에도 일반적으로 V가 양수가 되므로, 공격이 아님을 판별할 수 있다.

제안 기법은 이를 종합한 $((C < C_{min}) \vee (C \geq C_{min} \wedge N < N_{min} \wedge V \geq V_{min})) \Rightarrow Attack$ 규칙을 적용함으로써 위조 데이터 주입 공격을 판별한다. 특정 사건이 위조 데이터 주입 공격으로 판별된 이후에는, 공격자가 훼손한 노드들의 수를 C와 N을 기반으로 추정($C \times N$)하여 사용자에게 보고할 수 있다. 예를 들어, C = 100%, N = 5인 경우, 5개의 노드들이 훼손되었다고, C = 50%, N = 20인 경우, 10개의 노드들이 훼손되었다고 추정할 수 있다.

사용자는 제안 기법의 공격 탐지 보고를 바탕으로 적절한 조치를 취할 수 있다. 예를 들어, 소수의 노드가 훼손되었고 공격 트래픽의 양이 많지 않다면, SEF와 같은 가벼운 보안 기법을 활성화할 수 있다. 만약 공격 트래픽의 양이 전체 트래픽의 대부분을 차지한다면 KIF와 같은 조기 탐기 보안 기법을 적용할 수 있다. 훼손된 노드들의 수가 일정 이상인 경우에는, 해당 지역에 대응 인력을 투입하는 물리적인 방법을 활용할 수도 있다.

4. 시뮬레이션 결과

제안 기법을 검증하기 위하여 시뮬레이션을 수행하였다. 센서 노드 5,000개가 균일하게 배포된 1,000×100m^2 크기의 센서 필드를 사용하였으며, BS는 필드의 끝에 위치한다. 모든 노드는 이동 물체를 감지한 경우 매 2 단위 시간마다 감지 보고서를 생성하여 전달한다. 한 바이트의 전송/수신에는 16.25/12.5μJ을 소비하며, 하나의 MAC 생성에는 15μJ을 소비한다[8]. 원본 감지 보고서의 크기는 24바이트이며 하나의 MAC 크기는 1바이트이다. 각 이동 물체는 필드의 경계에서 나타난다. 물체는 단위 시간 당 U(5,10) 미터 속도로 이동하며 임의의 중간 지점들을 통과한다. 공격자는 DU(0,5)개의 노드들을 훼손할 수 있으며 DU(50,200)개의 위조 데이터들을 주입한다. 보고서 주입 간의 간격은 U(0.2,1)이다.

제안 기법의 평가 지표로는 위양성 비율과 위음성 비율이 사용되었다. 위양성 비율은 공격으로 판별된 사건들 중 위조 데이터 공격이 아니었으나 공격으로 판별된 사건들의 비율이며, 위음성 비율은 공격이 아닌 것으로 판별된 사건들 중 위조 데이터 공격인 사건들의 비율이다. 그림 6은 제안 기법에서 보고서 수집 시간 T에 따른 위양성 비율이다. 위양성은 주로 새로이 나타나거나 사라져가는 물체들에 기인한다. 그림에서 보는 바와 같이, T를 증가시

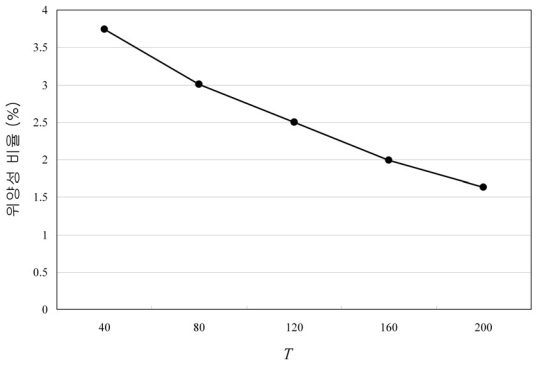

그림 6. 위양성 비율

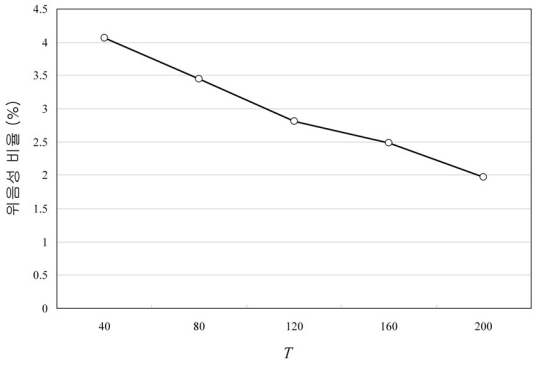

그림 7. 위음성 비율

킴에 따라 위양성 비율이 줄어든다. 이는 T를 늘릴수록 새로이 나타난 물체를 감지하는 노드들이 늘어날 확률($N \geq N_{min}$)이 증가하고, 사라져가는 물체의 경우, $V < V_{min}$ 일 확률이 증가하기 때문이다. 그러나 T의 증가는 제안 기법에서의 공격 탐지 시간과 공간 복잡도를 증가시킨다.

그림 7은 제안 기법에서 보고서 수집 시간 T에 따른 위음성 비율이다. 위양성에서와 같이, T 증가에 따라 위음성 비율이 줄어듦을 알 수 있다. 이는 수집 시간을 늘림에 따라 위조 데이터 공격의 서명이 명확하게 드러나고, 공격자가 실수할 가능성이 높아지기 때문이다.

5. 결론 및 향후 과제

본 논문에서는 이동 물체 추적을 위한 WSN에서 전달 과정 중 추가 에너지를 소비하지 않는 위조 데이터 주입 공격 탐지 기법을 제안하였다. 이를 위하여 먼저 시뮬레이션을 통하여 위조 데이터 주입 공격의 서명을 도출하였다. 제안 기법은 사건을 보고한 노드들의 수, 보고서들의 정확도, 보고한 노드들의 수 변화량을 기반으로 공격 여부를 판별하였다. 시뮬레이션을 통해 제안 기법이 대부분의 공격을 탐지할 수 있음을 보였으며, 보고서들이 버퍼에 저장되는 시간을 늘림에 따라 오류를 줄일 수 있음을 보였다. 위조 데이터 주입 공격이 탐지된 후에 기존의 보안 기법들을 가동시킨다면 보다 에너지 효율적으로 공격에 대응할 수 있을 것이다. 향후에는 제안 기법에서의 오류를 줄이기 위한 연구와 제안 기법에서 다루지 않은 공격들에 대한 공격 탐지 기법에 대한 연구를 수행할 계획이다.

참 고 문 헌

1. L. Buttyan, L. Dora, and I. Vajda, “Statistical Wormhole Detection in Sensor Networks,” Lecture Notes in Computer Science, Vol. 3813, pp. 128-141, 2005.
2. J.N. Al-Karaki and A.E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Communication Magazine, Vol. 11, No. 6, pp. 6-28, 2004.
3. W. Zhang and G. Cao, “Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach,” in Proc. INFOCOM, pp. 503-514, 2005.
4. S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” in Proc. S&P, pp. 259-271, 2004.
5. F. Li and J. Wu, “A Probabilistic Voting-Based Filtering Scheme in Wireless Sensor Networks,” in Proc. IWCMC, pp. 27-32, 2006.
6. H. Yang and S. Lu, “Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks,” in Proc. VTC, pp. 1223-1227, 2003.
7. F. Ye, 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, pp. 839-850, 2005.
8. Z. Yu and Y. Guan, “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” in Proc. SenSys, pp. 294-295, 2005.
9. H.Y. Lee and T.H. Cho, “Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks,” Lecture Notes in Computer Science 4371, pp. 116-127, 2006.
10. M.S. Kim and T.H. Cho, “A Multipath En-Route Filtering Method for Dropping in Sensor Networks,” IEICE Transactions on Information and Systems, Vol. E90-D, No. 12, pp. 2108-2109, Dec. 2007.

11. Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks,” IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 247-260, 2006.
12. H.Y. Lee and T.H. Cho, “Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks,” IEICE Transactions on Communications, Vol. E90-B, No. 12, pp. 3346-3353, 2007.
13. H. Tsai, C. Chu, and T. Chen, “Mobile Object Tracking in Wireless Sensor Networks,” Computer Communications, Vol. 30, No. 8, pp. 1811-1825, 2007.
14. http://www.xbow.com/
15. J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses,” in Proc. IPSN, pp. 259-268, 2004.

이 해 영 (sofware@swu.ac.kr)

2003 성균관대학교 정보통신공학부 공학사
2009 성균관대학교 컴퓨터공학과 공학박사
2009～현재 서울여자대학교 초빙강의교수

관심분야 : 설계 자동화, 임베디드 시스템, 모델링 시뮬레이션, 무선 센서 네트워크

조 대 호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 공학사
1987 University of Alabama 전자공학과 공학석사
1993 University of Arizona 전자 및 컴퓨터공학과 공학박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전사적 자원 관리