무선 센서 네트워크에서 PDoS 공격에서의 Compromised Node 탐지

윤영직○, 이광현, 홍충선
경희대학교 컴퓨터공학과
{yjyoon○, khlee}@networking.khu.ac.kr, cshong@khu.ac.kr

Detecting the Compromised Node in PDoS Attack on WSNs

Young Jig Yoon○, Kwang Hyun Lee, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University

요 약

PDoS (Path-based DoS) 공격은 J. Deng에 의해 처음 소개된 DoS 공격의 하나이다. PDoS 공격은 Base Station을 향해 대량의 bogus 패킷을 경로상에 플러딩하여 경로상에 있는 중간 노드들의 배터리 파워를 빠르게 소모를 시켜 수명을 단축시킨다. 그 결과 경로상의 중간 노드들은 수명을 마치게 되어 경로가 마비시켜 전체적으로 네트워크를 마비시킨다. 이런 PDoS 공격을 탐지하기 위해 J. Deng의 one-way hash function을 이용한 탐지방식은 매우 효율적이다. 하지만 공격자가 compromised node을 사용할 경우 이 탐지 기법은 소용이 없어진다.

compromised node는 특성상 특별하게 눈에 띄는 비정상 행위를 하지 않는 이상 일반 노드와 구분하기가 힘들며 공격자에 의해 다른 여러 공격에 이용되어 무선 센서 네트워크 보안에 큰 위협이 된다.

이에 본 논문에서는 무선 센서 네트워크상에서 PDoS 공격을 야기하는 compromised node를 탐지하는 방법을 제안한다.

1. 서 론

Path-based DoS(PDoS) 공격은 J. Deng[1] 에 의해 처음 소개된 DoS 공격의 하나이다. PDoS 공격은 공격자에 의해 대량의 bogus 패킷을 Base Station(BS)를 향해 경로상에 플러딩하여 경로 상에 있는 노드들의 빠른 배터리 소모를 유도하고 노드들의 수명을 단축시키는 공격이다.

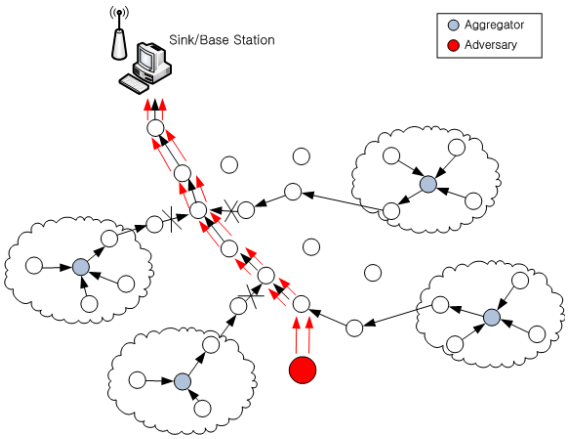


그림 1 무선 센서 네트워크에서의 PDoS 공격

그림1 은 무선 센서 네트워크상에서의 PDoS 공격을 보여준다. 그림1 에서 공격자는 일반적인 패킷이 흐르는 경로 상에 대량의 패킷을 플러딩하고 이 대량의 패킷들은 경로상의 노드들을 거쳐 BS로 전송된다.

이 과정에서 경로 상에 있는 중간 노드들은 대량의 패킷들로 인해 많은 양의 배터리 파워를 소모하게 되어 수명이 빠르게 단축된다. 또 대량의 패킷을 포워딩하는데 모든 자원을 집중하게 되어 주변의 다른 클러스터의 aggregator가 BS로 보내는 패킷을 제대로 포워딩 할 수 없게 된다. 결국 계속된 PDoS 공격으로 인해 경로상의 노드들은 주변의 다른 노드와 통신을 할 수 없게 되고 심각한 에너지 소비로 인해 몇 개의 노드들이 수명을 마침으로써 경로는 마비되게 된다.

이와 같은 PDoS 공격의 피해를 막기 위해 J. Deng은 one-way hash function을 이용한 경량화된 탐지 기법[1]을 제시하였다. 이 탐지 기법에서 공격자는 사전에 주어진 hash function을 가지고 있지 않기 때문에 next OHC number를 생성할 수 없으므로 쉽게 탐지가 된다. 하지만 만약 공격자가 hash function을 가지고 있는 노드를 compromise 할 경우 문제는 심각해진다.

* "본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음"(IITA-2008-(C1090-0801-0016))

compromise 된 노드는 hash function을 가지고 있기 때문에 제시된 탐지기법이 적용되지 않으며 compromised node의 특성상 특별하게 눈이 띄는 비정상 행위를 하지 않는 이상 일반 노드와 구분하기가 힘들다. 이런 compromised node는 무선 센서 네트워크상에서 공격자에 의해 여러 공격에 이용될 수 있고 탐지가 어려워 센서 네트워크 보안에 큰 위협이 된다.

이에 본 논문에서는 무선 센서 네트워크 상에서PDoS 공격을 야기하는 compromised node를 탐지하는 방법을 제안한다.

본 논문은 다음과 같이 구성되었다. 2장에서는 compromised node의 위험성과 제안된 탐지 방법의 관련 연구들에 대해 설명한다. 3장에서는 본 논문에서 제안하는 PDoS 공격을 야기하는 compromised node을 탐지하는 방법에 대해 설명한다. 마지막으로 결론과 향후 과제에 관하여 언급한다.

2. 관련연구

2.1 Compromised Node의 위협성

센서 노드는 값이 싸고 tamper-proof 장치가 없기 때문에 공격자에 의해 쉽게 compromise될 수 있다. 이렇게 compromise 된 node의 모든 정보와 권리는 공격자가 가진다. 이에 compromised node는 일반 노드 사이에 있을 경우 특별하게 비정상 행위를 하지 않는 한 일반 노드와 구분하기가 매우 힘들다.

또한, compromised node는 공격자에 의해 여러 계층에서 공격을 야기한다. 예를 들어, compromised node는 공격자에 의해 물리층에서 전송 채널을 jamming하거나 MAC층에서는 random backoff 메커니즘을 조작하여 다른 노드들의 수명을 마치게 할 수 있다. 또 네트워크층에서는 라우팅 메시지를 드랍하거나 변경 재전송을 할 수도 있으며, 응용층에서는 false alarm을 유발하는 false data를 리포트할 수 있다.

이와 같이, compromised node는 무선 센서 네트워크의 보안에 큰 위협이 되며 이를 탐지하는 것이 다른 공격 탐지에 있어서도 중요하다고 할 수 있다.

2.2 OHC(One-way Hash Chain)를 이용한 탐지 기법 [1][2]

J. Deng이 제안한 이 방법은 one-way hash의 장점을 이용한 탐지 기법이다. 이 탐지 기법에서 모든 노드들은 사전에 hash function을 가지고 있으며 hash function에 의해 OHC number를 생성하게 된다.

그림2 는 one-way hash chain을 이용한 PDoS 공격을 탐지하는 것을 보여준다.

각 source node들은 자신만의 one-way hash chain HS : $\langle HS_n, HS_{n-1}, \cdots, HS_1, HS_0\rangle$을 가지고 있다. source node가 패킷들을 BS로 전송할 때 각 패킷들은 OHC sequence number를 가진다. 예를 들어 첫 번째 패킷일 경우 패킷에 HS_1을 가지고 두 번째 패킷의 경우 HS_2를 가진다. 이렇게 전송되어지는 패킷들은 중간 노드들에서 $Vs=F(HS_i)$을 성립할 경우 통과를 하게 되고 아닐 경우 패킷은 버려진다.

공격자는 hash function을 가지고 있지 못하므로 Next OHC number를 생성할 수 없으며 중간 노들의 검증과정에서 쉽게 발견되어지며 패킷은 버려진다.

하지만 이 공격 기법에서는 공격자가hash function을 모를 경우에 적용이 가능한 기법이다. 만일 공격자가 hash function을 가지고 있는 노드를 compromise한 후 이 노드를 이용하여 공격을 할 경우 중간 노드들의 검증과정에서 발견되어 지지 않는다.

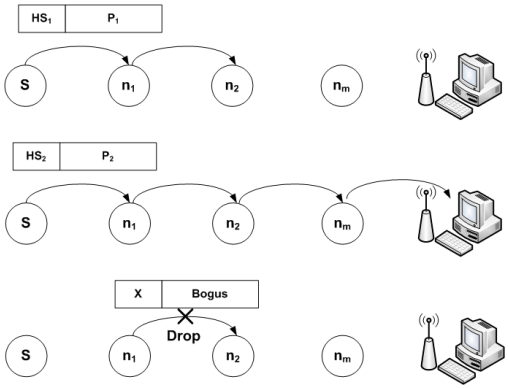


그림 2 One-way hash chain을 이용한 PDoS 공격

2.3 Mobile Agent를 이용한 PDoS 공격에서 compromised node 탐지[3][4]

이 방식은 Mobile Agent[3]를 이용하여 PDoS 공격을 탐지하는 기법이다. Mobile agent는 고성능의 하드웨어로서 센서 네트워크 내를 이동하면 일정 범위 내에 있는 센서들의 정보를 수집한다. 센서는 특성상 제한된 자원을 가지고 있기 때문에 이웃의 정보를 저장하거나 상위 노드로 전송하는 것이 힘들기 때문에 센서를 대신하여 Mobile Agent에서 센서들의 정보를 수집한다. 이를 통해 센서들의 에너지와 네트워크의 오버헤드를 줄일 수 있다.

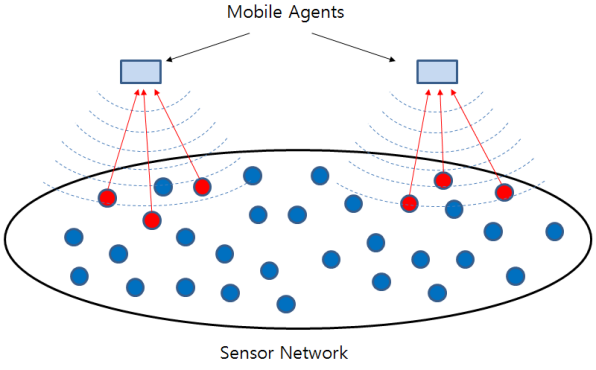


그림 3 센서 네트워크에서의 Mobile Agent

이런 Mobile Agent의 특징을 이용하여 이 기법에서는 센서 노드들의 정보를 Mobile Agent에서 수집하고 센서 노드들을 대신하여 PDoS 공격 탐지 알고리즘을 수행하게 된다. 이 경우 센서 노드들의 에너지와 오버헤드를 줄일 수 있다.

하지만 센서 노드들의 전송 범위가 짧고 범위가 큰 네트워크일 경우 Mobile Agent를 이용하기가 매우 힘들다는 단점이 있다.

3. 제안사항

3.1 네트워크 모델

본 논문에서는 탐지 기법을 위하여 다음의 몇 가지를 가정한다.

1. 무선 센서 네트워크의 토폴로지로 트리구조를 사용하며 하나의 BS를 가진다.
2. BS와 중간 노드들은 공격자에 의해 compromise되지 않는다.
3. 각 노드를 구분하기 노드들은 고유한ID를 가지며 자신의 이웃 노드들의 정보를 알고 있다
4. compromised node는 다른 노드들에게 올바른 정보를 전달하지 않는다. (Byzantine General Problem[5])

3.2 탐지 기법

본 논문에서 제안하는 탐지 기법은 그림 에서와 같이 크게 두 파트로 나눠진다.

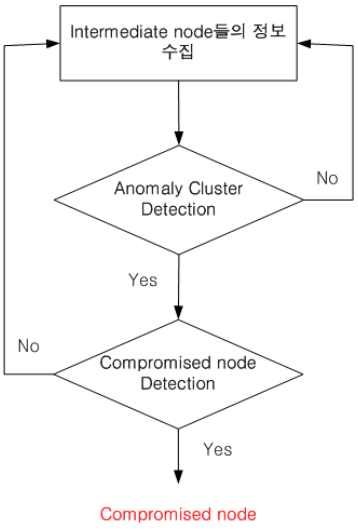
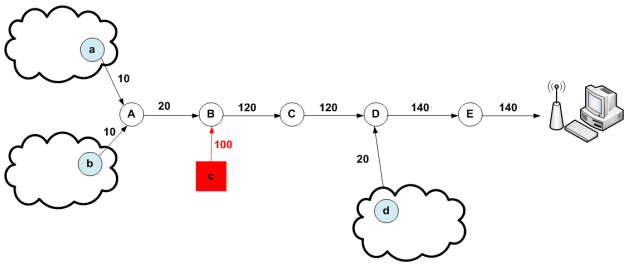


그림 4 Compromised node 탐지 기법

3.2.1 비정상 Cluster 탐지

비정상 cluster 탐지에서는 각 cluster의 aggregator로부터 중간노드로 들어오는 패킷들의 수를 모니터링하여 cluster의 이상 유무를 탐지한다.

다음의 그림5는 비정상 cluster 탐지 과정을 보여준다.



Node	패킷을 보낸 노드	받은 패킷의 수	
A	a,b	20	20
B	c	120	100
C		120	0
D	d	140	20
E		140	0

그림 5 비정상 cluster 탐지

각 중간 노드에서는 유인되는 패킷들을 보내는 노드의 ID와 유입된 패킷의 총 수를 주기적으로BS에게 전송한다. 이 때 중간 노드들은 단순히 패킷의 총 수를 카운팅만 할 뿐 다른 일은 하지 않는다. BS에서는 중간노드들이 전송한 정보를 토대로 그림5에서의 표를 만든다.

BS는 중간 노드에 유입된 패킷의 총 수에서 이전 중간 노드로부터 유입된 패킷의 수를 차감함으로써 중간 노드에 유입되는 cluster의 패킷 수를 알게 되고 만약 cluster의 패킷의 수가 사전에 정한 임계치 값을 초과할 경우 비정상 cluster로 간주한다.

3.2.2 Compromised Node 탐지

비정상 cluster 탐지를 통하여 비정상 cluster로 탐지되었다고 하여 이 cluster가 compromised node에 의한 공격이라고 간주할 수는 없다. 그것은 센서 노드가 오작동을 했을 수도 있으며 실제로 cluster 내에서 전송할 데이터가 많아 순간적으로 패킷의 양이 많을 수도 있기 때문이다. compromised node 탐지에서는 이런 이유로 인해 실제 이 compromised node가 있는 cluster인지 여부를 판별한다.

다음의 그림6 은 compromised node를 판별하는 과정을 보여준다.

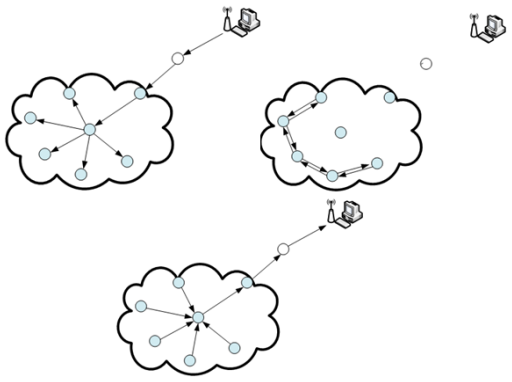


그림 6 Compromised node 탐지

BS는 cluster 내에 compromised node의 존재 여부를 판별하기 위해 비정상 cluster로 탐지된 cluster로 랜덤한 메시지를 전송한다. 메시지를 받은 중간 노드는 이 메시지를 cluster의 aggregator로, aggregator는 메시지를 하위의 노드로 전송하며, 하위 노드들은 다시 이 메시지를 자신의 이웃 노드들에게 전송한다. 이 후 하위 노드들은 aggregator로부터 받은 메시지의 정보와 이웃 노드들이 보낸 메시지의 정보를 비교하여 그 결과를BS로 다시 전송하게 된다.

만약 cluster 내에 compromised node가 있다면 BS로부터 메시지를 전송 받은 후 다른 메시지로 변조하여 이웃 노드들에게 전송[5]하게 되며 그 결과 하위 노드가 BS로 재전송한 결과와 BS가 cluster로 보낸 메시지가 서로 다를 것이다. 이와 반대로 compromised node가 없다면 하위 노드가 전송한 결과와BS가 전송한 메시지의 정보는 같을 것이다.

다음의 그림들은 compromised node 탐지의 예를 보여준다.

그림7 에서와 같이 aggregator가 compromised node일 경우 모든 하위 노드들은 BS가 전송한 M이라는 메시지 대신 aggregator에 의해 변조된 정보인 X라는 메시지를 전송받게 된다.

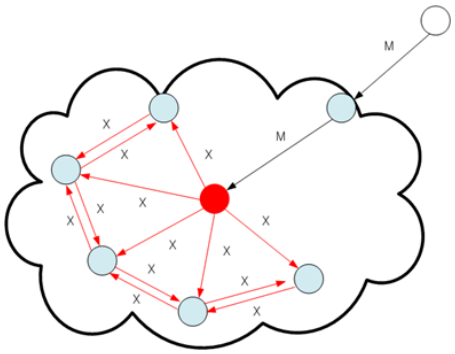


그림 7 Aggregator가 Compromised node일 경우

그림8 은 하위 노드가 compromised node 일 경우 compromised node의 이웃 노드들은 BS가 전송한 M이라는 메시지 대신 compromised node가 전송한 변조된 X라는 메시지를 받게 될 것이다.

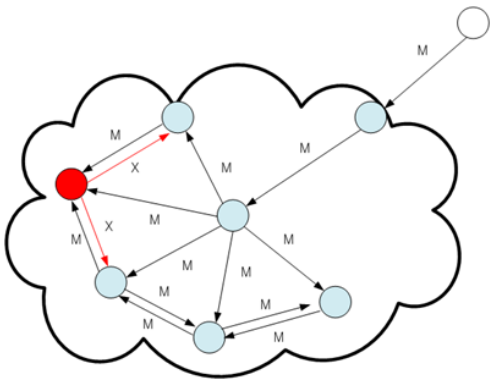


그림 8 하위 노드가 compromised node일 경우

4. 결론 및 향후 연구

본 논문에서는 PDoS 공격에서의 compromised node를 탐지하는 방법을 제안하였다. PDoS 공격은 대량의 패킷을 플러딩하여 경로를 마비시켜 나아가 전체 네트워크를 마비시키는 매우 위협적인 공격이다.또한 이런 위협적인 PDoS 공격이 탐지하기가 어려운 compromised node에 의해 발생되었을 경우 탐지가 되지 않아 그 피해가 클 것이다. 그러므로 compromised node를 탐지하는 것이 어느 공격에 있어서든 매우 중요하다고 할 수 있다. 이를 위해 본 논문에서는 네트워크의 트래픽 모니터링을 통하여 PDoS 공격에서의 compromised node를 탐지하는 기법을 제안하였다.

향후 과제로는 본 논문에서 제안된 탐지 기법에 대한 보안성 및 성능 분석을 통하여 제안 사항을 검증하고 이를 통해 제안된 탐지 기법을 개선하여 실제 무선 센서 네트워크에 안정적으로 사용이 가능하도록 해야 할 것이다.

5. 참고문헌

[1] J. Deng et al., “Limiting DoS attacks during multihop data delivery in wireless sensor networks“, International Journal of Security and Networks, Vol. 1, No.3/4 pp. 167 - 178, 2006

[2] Peng Ning, “Mitigating DoS Attacks against Signature-Based Broadcast Authentication in Wireless Sensor Networks“, ACM journal no.20, 2005

[3] Tong L., Zhao Q., and Adireddy S., “Sensor networks with mobile agents,” in Proceeding Military Communications Int Symp., pp. 688-693, Oct. 2003,

[4] Bai Li, Lynn Batten, “ Using Mobile Agents to Detect Node Compromise in Path-Based DoS Attacks on Wireless Sensor Networks “, WiCom(Networking and Mobile Computing, 2007) 2007. 21-25 Sept 2007

[5] Lamport, L., Shostak, R., and Pease, M., “The Byzantine Generals Problem.”, ACM Trans. Program. Lang. Syst. 4, 3 (Jul. 1982), 382-401.