www.kics.or.kr

2013년도 한국통신학회 하계종합학술발표회 프로그램

|일시| 2013년 6월 19일(수) ~ 21일(금)

|장소| 라마다프라자 제주호텔 2층

|주최| 한국통신학회

|협찬| 삼성전자, SK텔레콤, LG U+, KT, Ericsson-LG, LG전자, Qualcomm, 넷비젼텔레콤, ㈜엠에이

KICS
한 국 통 신 학 회

협력적 무선 다중 접속 망에서 네트워크 부호를 이용한 릴레이 공격 감지 방법

이웅비, 강주성, J. Oliver, 이흥노*
광주과학기술원

wblee@gist.ac.kr, k92492@gist.ac.kr, oliver@gist.ac.kr, *heungno@gist.ac.kr

Attack Detection in the Cooperative Wireless Multiple Access Networks

Lee Woong Bi, Kang Ju Sung, J. Oliver, Lee Heung No*
School of Information and Communications
Gwangju Institute of Science and Technology

요 약

본 논문은 협력적 무선 다중 접속 망에서 네트워크 부호의 오류 정정 특성을 이용하여 무선 릴레이들에 임의의 확률로 가해질 수 있는 공격을 액세스 노드(Access Node) 에서 사전정보 없이 감지하는 방법에 대해서 연구하였다.

Ⅰ. 서 론

릴레이를 이용하여 협력적 무선 네트워크 부호를 사용하는 무선 다중 접속 망 (Wireless Multiple Access Network, WMA Network)은 센서 네트워크 등 다양한 분야에서 큰 주목을 받고 있다 [1][2]. 무선 다중 접속 망은 두 단계로 이루어져 있는데, 첫 단계에서는 각각의 소스 노드(Source Node)들이 액세스 노드(Access Node)로 메시지들을 전송한다. 이 때, 무선 통신의 특징에 따라서 릴레이 노드(Relay Node)들이 몇몇의 소스 노드들이 전송한 데이터를 수신하게 된다. 두 번째 단계에서는 각각의 릴레이들이 수신한 소스 노드의 데이터들을 네트워크 부호화, 즉 패러티 검사(Parity Check)를 하여 그 결과를 액세스 노드에 전송을 하게 된다. 이러한 부호화 방법을 무선 다중 접속망(WMA)의 네트워크 부호라고 한다 [3][4]. 네트워크 부호화를 통한 소스 노드와 릴레이 노드의 협력 과정들을 통해서 보다 더 신뢰성이 있는 통신 환경을 만들 수 있다.

이러한 협력적 무선 네트워크 부호화는 릴레이들의 신뢰성을 바탕으로 이루어진다. 하지만 무선 환경의 릴레이들은 외부로부터의 접근이 용이하기 때문에 외부로부터의 공격에 취약하다. 따라서, 무선 릴레이들에 대한 신뢰성이 무너지게 된다면 전체 네트워크 성능에 큰 악영향을 끼치게 된다 [5].

[5]에서는 네트워크 부호화를 이용한 무선 다중 접속망의 보안 메커니즘을 다루었는데, 각 릴레이들에 대한 공격 확률이 모두 동일하고, 액세스 노드가 공격자에 대한 사전 정보를 가지고 있다는 문제가 있다. 본 논문에서는 액세스 노드가 공격자에 대한 사전 정보가 없을 때, 그리고 릴레이 공격 확률이 서로 동일하지 않는 경우에도 액세스 노드가 공격받는 릴레이들을 검출할 수 있는 방법에 대해 기술한다.

본 논문의 구성은 2 장에서 무선 네트워크 부호를 사용하는 무선 다중 접속망에서 임의의 릴리에 노드에 공격이 가해지는 경우를 모델링하고, 공격 감지 방법에 대해서 기술한다. 3 장에서는 컴퓨터 모의실험 환경과 릴레이 공격을 검출결과를 보였고, 4 장에서는 논문의 결과를 정리하였다.

Ⅱ. 본론

2.1 릴레이 공격이 존재하는 협력적 무선 다중 접속 망 모델링

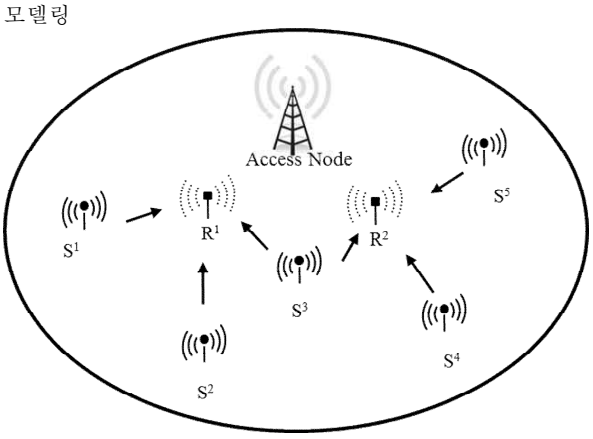

그림 1. 협력적 무선 다중 접속 망

협력적 네트워크 부호를 사용하는 무선 다중 접속망은 그림 1 과 같이 나타난다. 첫 번째 단계에서는 N_s 개의 소스 노드가 신호를 액세스 노드로 전송하게 되고, N_r 개의 릴레이 노드들은 몇몇의 소스 노드들로부터 전송된 신호를 수신하게 된다. 두 번째 단계에서는 릴레이 노드들이 수신한 소스 노드 데이터를 부호화하여서 그 결과를 액세스 노드로 전송하게 된다. 이러한 두 단계를 거쳐서 네트워크 부호를 형성하게 된다.

네트워크 부호를 생성하는 릴레이 노드는 무선 통신 환경의 특성에 따라서 재밍공격과 같은 외부로부터의 공격 또는 접근이 용이하게 된다. 외부로부터 공격을 받은 릴레이 노드에서 네트워크 부호화가 된 데이터와 상반된 데이터를 액세스 노드에 전송한다면, 네트워크 부호를 복호화 하는 과정에서 소스 메시지와 릴리에 메시지들의 상관관계 때문에 많은 오류가 발생하게 된다.

이러한 릴레이 공격이 서로 다른 확률로 있는 경우 액세스 노드에서 공격자에 대한 사전 정보가 없을 때, 공격하는 릴레이들을 감지하는 방법에 대해서 알아본다.

2.2 릴레이 공격 감지 방법

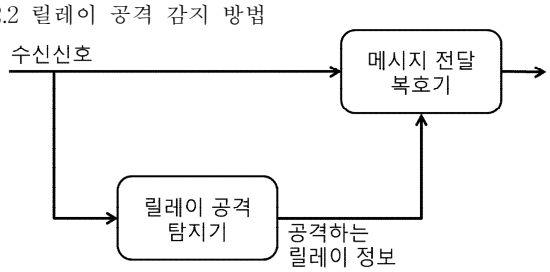

그림 2. 릴레이 공격 탐지 및 이용방법

본 논문에서는 네트워크 부호를 복호하기 위해서 메시지 전달 복호기를 고려한다. 메시지 전달 복호기는 반복되는 과정을 통해서 채널에 의해 발생한 오류를 정정하게 된다. 릴레이 노드로부터 수신된 데이터를 외부 공격에 의해 신뢰할 수 없다고 할 때, 릴레이 노드로부터 수신된 데이터의 메시지 전달 복호기로의 입력과 출력을 일정 시간 동안 관찰한다면 릴레이 공격 여부를 판단할 수 있다. 즉, 릴레이 공격이 있는 경우는 메시지 전달 복호기는 공격받은 릴레이 데이터를 반복되는 복호 과정을 통해서 정정을 하게 된다. 따라서, 공격을 받은 릴레이의 데이터를 일정 시간동안 관찰하게 되면 오류 정정 빈도가 공격받지 않은 릴레이에 비해 현저하게 높게 나타나게 된다. 이를 수학적 분석을 통해서 공격받는 릴레이 빈도의 최소값과 최대값을 구할 수 있고, 그 구간에서 공격받는 릴레이와 일반 릴레이의 임계값을 구할 수 있다. 임계값을 통해 공격하는 릴레이와 일반 릴레이를 구분하고, 그 정보를 그림 2 에서처럼 메시지 전달 복호기에 적용하여서 신뢰성이 낮은 릴레이로부터의 정보를 메시지 전달 복호 과정에서 배제시킴으로써 네트워크 신뢰도의 악화를 감소 시킬 수 있다.

Ⅲ. 컴퓨터 모의실험

그림 3 은 100 개의 소스 노드가 100 개의 릴레이 노드의 협력으로 액세스 노드와 통신을 하는 환경이다. 그림 3 (a)는 15 개의 릴레이 노드가 동일한 확률, 0.5 로 공격을 하는 경우, (b)는 5 개의 릴레이가 0.3, 5 개의 릴레이가 0.5. 나머지 5 개의 릴레이가 1.0 의 확률로 공격을 하는 경우를 나타낸다. 그림에서 볼 수 있듯이, 공격받는 릴레이와 공격받지 않는 릴레이의 메시지 전달 복호기의 입력과 출력이 다른 횟수가 현저하게 다른 것을 볼 수 있다. 또한, 제안하는 방법을 통해서 공격하는 릴레이와 일반 릴레이를 확연하게 구분할 수 있는 것을 볼 수 있다.

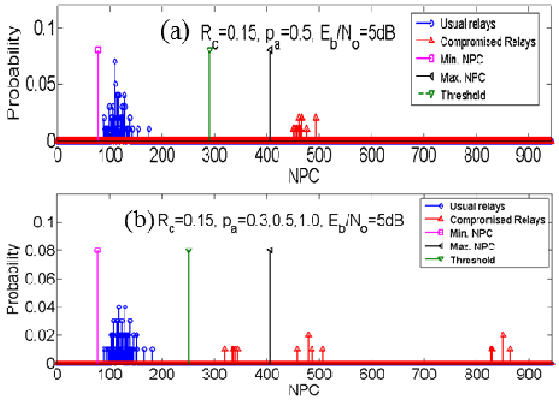

그림 3. (a) 릴레이 공격이 서로 같은 확률일 경우, (b) 릴레이 공격이 서로 다른 확률일 경우

Ⅳ. 결론

본 논문에서는 협력적 네트워크 부호화를 사용하는 무선 다중 접속 망 환경에서 외부로부터의 공격에 취약한 무선 릴레이들이 잘못된 네트워크 부호 정보를 임의의 확률로 전송하는 경우, 액세스 노드에서 사전정보 없이 공격하는 릴레이 노드들을 감지하는 방법을 연구하였다.

ACKNOWLEDGMENT

이 논문은 2012 년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (중견연구자-도약연구사업, NO. 2012-0005656)

이 논문은 2012 년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (중견연구자-핵심연구사업, NO. 2012-047744)

참 고 문 헌

[1] X. Bao and J. Li, "Matching code-on-graph with network-on-graph: adaptive network coding for wireless relay networks," in Proc. Allerton Conf. on Commun., Control and Computing, Urbana Champaign, IL, Sept. 2005.

[2] C.-C. Chang and H.-N. Lee, "Space-time mesh codes for the multiple-access relay network: space v.s. time diversity benefits, "in Proc. Inform. Theory and Applications Workshop(ITA), San Diego, CA, Jan. 2007.

[3] J.L. Laneman, D.N.C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," IEEE Trans. Inform. Theory, vol. 50. 12, pp. 3062-3080, Dec. 2004.C.-C.

[4] E.Ayanoglu, C.-L. I, R. D. Gitlin, and J.E. Mazo, "Diversity coding for transparent self-healing and fault-tolerant communication networks," IEEE Trans. Communications, vol. 41, no. 11, pp. 1677-1685, Nov. 1993.

[5] 이웅비, 최재건, 이홍노, " 무선 다중 접속 망에서의 네트워크 부호를 이용한 보안 메커니즘" , 한국통신학회 하계학술대회, 2011