무선 다중 접속 망에서의 네트워크 부호를 이용한 간단한 보안 메커니즘

이웅비, *이흥노
광주과학기술원 정보통신공학부
e-mail : wblee@gist.ac.kr, *heungno@gist.ac.kr

A simple Security Mechanism using Network Codes for Wireless Multiple Access Network

Woong-Bi Lee, *Heung-No Lee
School of Information and Communications
Gwangju Institute of Science and Technology

Abstract

In WMA(Wireless Multiple Access) networks, two-phase relay transmission with network coding is widely studied due to its robust performance. However, relay nodes located in open fields are exposed to external attacks, and some attacked relay nodes can make fatal attacks to whole network communications. This paper proposes a simple security mechanism which can find out attacked indices of relay nodes by using network codes.

I. 서론

두 단계로 구성되는 무선 다중 접속 망(Wireless Multiple Access Networks, WMA)에서 네트워크 부호는 최근 크게 주목을 받고 있다[1][2]. 첫 번째 단계에서는 소스 노드에서 액세스 노드로 전달한 정보를 각각의 릴레이 노드에서 듣고 패러티 검사를 하게 된다. 두 번째 단계에서는 각 릴레이 노드에서 수행한 패러티 검사를 access 노드로 전송을 하게 된다. 이러한 부호화 방법을 무선 다중 접속(WMA) 네트워크 부호라고 하고, 이러한 환경의 네트워크를 WMA 네트워크라고 한다.[3][4] 네트워크 부호화는 소스 노드와 릴레이 노드가 서로 협력을 함으로써 안정된 통신 환경을 만들 수 있다.

하지만 네트워크 부호화가 된 통신 환경에서 개방된 공간에 위치한 릴레이 노드가 누군가로부터 공격을 받아 잘못된 패러티 검사 정보를 전송하게 된다면 전체 시스템 성능에 큰 악영향을 끼치게 된다.

본 논문에서는 WMA 환경에서 임의의 릴레이 노드가 누군가로부터 공격을 받아 잘못된 패러티 검사 정보를 전송 할 때, 네트워크 부호화 방법을 이용하여 공격을 받고 있는 릴레이 노드의 위치를 쉽게 찾아낼 수 있는 방법에 대해 기술한다.

본 논문의 구성은 2장에서 두 단계 네트워크 모델링 하고 임의의 노드에 공격이 가해졌을 때 액세스 노드에서 공격을 검출하는 방법에 대해 기술한다. 3장에서는 컴퓨터 모의실험 환경과 결과를 보였고, 4장에서 결론을 내었다.

---

1) * 교신저자

2) This work was supported by the Korea National Research Foundation (NRF) Grant K20901000004-09E0100-00410.

II. 본론

2.1 네트워크 모델링

두 단계의 릴레이 협력 네트워크 부호화 모델은 그림 1에서와 같이 구성하였다. K개의 소스 노드가 신호를 액세스 노드로 전달하는데 L개의 relay nodes가 있어서 통신을 도와주게 된다. 이러한 K/(L+K)의 부호화율을 갖는 네트워크 코드는 두 단계로 이루어져 있다. 첫 번째 단계에서는 소스 노드에서 액세스 노드로 정보를 그들의 직교채널을 통해서 전송하게 된다. 이 때, 무선 통신의 전파 전달 특성 때문에 릴레이 노드들은 몇몇의 소스에서 전송한 메시지를 받고 복호화하게 된다. 두 번째 단계에서는 릴레이 노드에서 받고 복호화한 정보들을 패러티 검사를 하여 액세스 노드로 패러티 비트를 보내게 된다.

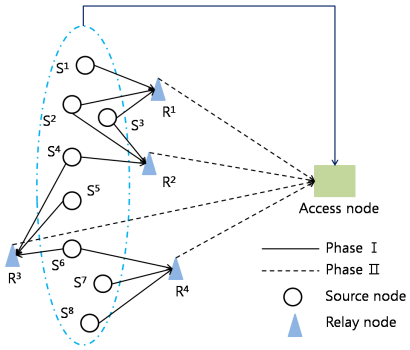

그림 1. Wireless multiple access relay network의 예

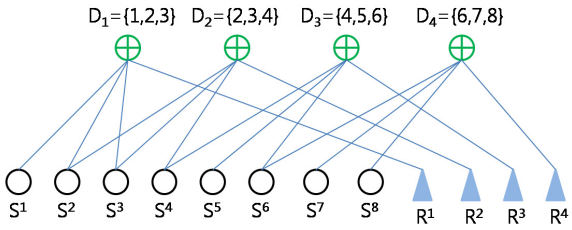

그림 2. 그림 1의 그래프 코드

그림 2는 그림 1에서 예로 들은 WMA 환경의 그래프 코드를 나타낸다. 액세스 노드에서는 그림 2와 같이 부호화 된 정보들의 LLRs(log-likelihodd ratios)를 취해서 원래의 소스 정보들을 복호화 하게 된다. LLRs를 가지고 복호화 과정을 일정한 숫자 이상 반복하게 되면 서로 독립된 정보들이 복호화 된다. 이러한 공간 영역에서의 부호화는 큰 부호화(coding) & 다이버시티(diversity) 이득을 가져다준다.

2.2 공격을 감지하는 검파 방법

릴레이 노드에 공격이 가해지지 않고 신호 대 잡음비가 큰 채널을 가정하면 액세스 노드의 복호기의 입력과 출력의 부호가 다를 확률은 크지 않다. 이 채널에서 릴레이 노드에 공격이 가해져서 정 반대의 패러티 검사 비트를 전송하게 되면 복호기의 입력 부호가 반대가 된다. 하지만 반복적으로 복호화하는 과정에서 출력 부호는 원래의 부호를 갖게 된다. 따라서 일정 기간 동안 복호기의 입력과 출력의 부호가 서로 다른 노드들의 평균값(Average Suspicious Index, ASI)를 관찰하면 공격이 가해지는 릴레이 노드의 위치를 파악할 수 있다.

III. 컴퓨터 모의실험

컴퓨터 모의실험은 100개의 소스 노드와 100개의 릴레이 노드 환경에서 수행하였다. 모든 소스와 릴레이 노드들이 액세스 노드로부터 동일한 거리에 위치해 있다고 가정함으로써 각각의 채널의 noise variance는 동일하다고 여겼다.

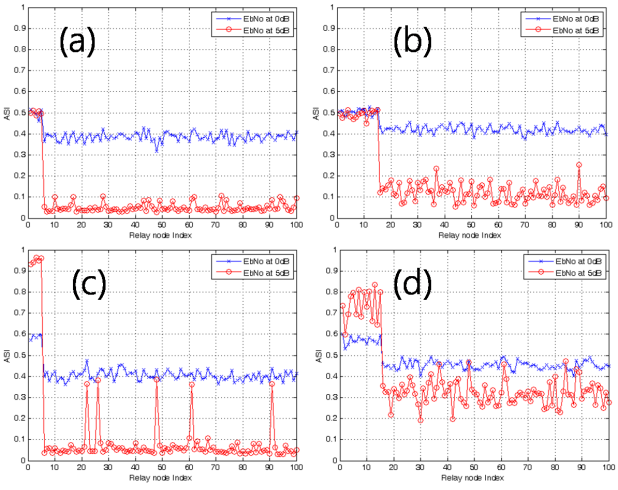

그림 3. Average suspicious

probability / density	0.5	1.0
5%	(a)	(c)
15%	(b)	(d)

표 1. 모의실험 파라미터

그림 3은 전체 릴레이노드의 5%와 15%가 공격을 받는 경우 1000개의 샘플들에 대한 Average suspicious 를 나타내다. 비트대 잡음비(Eb/No)이 0dB와 5dB인 환경에서 (a), (c)는 1~5, (b), (d)는 1~15 릴레이 노드가 공격을 받아서 패러티 검사와 반대 되는 비트를 전송하였다. 대부분의 경우에서 공격을 받은 릴레이 노드들의 ASI는 공격을 받지 않은 릴레이 노드들에 비해 값이 크다. 따라서 낮은 Eb/No의 환경에서도 액세스 노드에서 공격을 받아 잘못된 정보를 전송하는 릴레이 노드들의 위치를 정확히 파악할 수 있다. 하지만 15%의 릴레이 노드들이 공격을 받는 경우의 ASI 값은 공격을 받지 않은 릴레이 노드들의 ASI 값과 크게 차이가 나지 않기 때문에 정확한 위치를 찾는 게 어렵다고 하겠다. 그러므로 전체 릴레이 노드의 15% 이상이 공격을 받는다면 전체 네트워크가 크게 손상을 입는다고 할 수 있다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 무선 네트워크 통신 환경에서 소스 노드와 릴레이 노드가 협력하여 네트워크 부호화를 하면 임의의 릴레이 노드들이 누군가로부터 공격을 받아 잘못된 패러티 검사 비트를 전송하는 경우 액세스 노드에서 공격을 받고 있는 릴레이 노드의 위치를 간단하게 파악할 수 있음을 알아보았다.

참고문헌

[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.

[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.