무선 다중 접속 망에서의 네트워크 부호를 이용한 보안 메커니즘

이웅비, 최재건, *이흥노
광주과학기술원 정보기전공학부

wblee@gist.ac.kr, jgchoi@gist.ac.kr, *heungno@gist.ac.kr

A Security Mechanism using Network Codes for Wireless Multiple Access Network

Woong-Bi Lee, Jae-Gun Choi, *Heung-No Lee
School of Information and Communications

Gwangju Institute of Science and Technology

요 약

본 논문은 두 단계로 구성되는 협력적 네트워크 부호화를 이용하는 무선 다중 접속 망의 보안성문제를 연구하였다. 협력적 네트워크 부호화는 네트워크 성능 향상을 가져다 주지만, 릴레이 공격에 취약하고, 적은 수의 릴레이 공격에도 네트워크 성능은 크게 저하된다. 따라서 본 논문에 서는 무선 다중 접속 망에서 협력적 네트워크 부호화를 사용할 때, 공격 당하는 릴레이들을 찾아내고 보상하는 방법에 대해서 연구하였다

Ⅰ. 서 론

두 단계로 구성되는 협력적 무선 네트워크 부호를 이용한 무선 다중 접속 망 (Wireless Multiple Access Networks, WMA)은 최근 크게 주목을 받고 있다[1][2]. 두 단계의 협력적 무선 네트워크는 다음과 같이 구성된다. 첫 단계로 각각의 소스 노드가 액세스 노드로 메시지를 전송한다. 이 때, 무선 통신의 특성에 의해서 릴레이 노드들이 몇몇의 송신된 메시지들을 수신하게 된다. 두 번째 단계에서는 릴레이 노드들이 수신한 메시지들을 네트워크 부호화하여 액세스 노드로 전송하게 된다. 이러한 협력적 무선 네트워크 부호를 이용함으로써 전체 네트워크 시스템의 성능을 향상시킨다.

하지만 협력적 무선 네트워크는 릴레이들의 신뢰성을 바탕으로 이루어 지는데, 네트워크 부호화를 사용하는 통신 환경에서 개방된 공간에 위치한 릴레이 노드는 외부의 공격으로부터 취약하고, 이로 인해 잘못된 부호화 정보를 액세스 노드에 전송하게 된다면 전체 시스템 성능에 큰 악영향을 끼치게 된다.

본 논문에서는 외부에서의 공격을 받는 WMA 네트워크 환경에서, MP (message-passing) 복호기에 간단한 알고리즘을 추가하여 공격을 받는 릴레이 노드들을 찾아내고, 이를 보상하는 방법에 대해 기술한다.

본 논문의 구성은 2 장에서 네트워크 모델링과 두 단계의 전송 과정을 나타내었고, 임의의 릴레이 노드에 공격이 가해졌을 때 액세스 노드에서 공격을 검출 및 보상 방법에 대해 기술을 하였다. 3 장에서는 컴퓨터 모의 실험결과를, 4 장에서 논문의 결과를 정리 하였다.

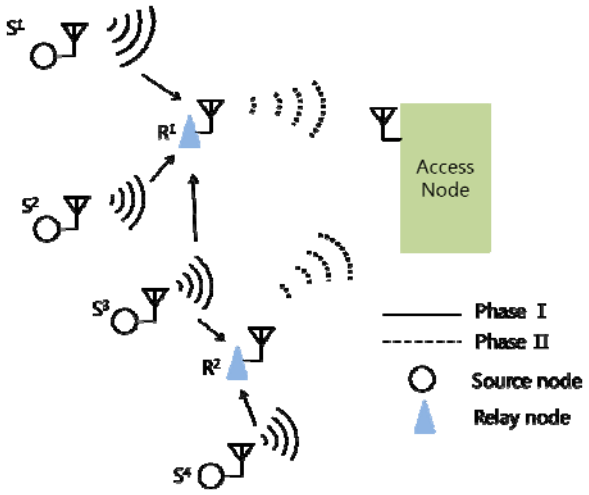

그림 1. 협력적 네트워크 부호화를 사용하는 Wireless Multiple Access Network 의 예

Ⅱ. 본론

2.1 네트워크 모델링

두 단계를 갖는 협력적 네트워크 부호화는 그림 1 에서와 같이 나타난다. 첫 번째 단계에서, N_S 개의 소스 노드들이 액세스 노드로 데이터를 전송하고 무선통신의 특성에 의하여 근처에 위치한 N_R 개의

릴레이들이 일부의 데이터를 수신하게 된다. 두 번째 단계에서는, 각각의 릴레이 노드들이 수신한 메시지를 부호화하여 액세스 노드로 전송하게 된다. 이 두 단계를 거쳐서 네트워크 코딩을 형성하게 되는데, 이를 LDGM (low density generator matrix)라고 한다[3][4].

이러한 네트워크 코딩은 네트워크 성능을 크게 향상시키지만, 릴레이 노드들의 신뢰성이 확보되지 않다면 네트워크 성능에 악영향을 끼치게 된다. 따라서 이러한 공격을 감지하고 보상하는 방법에 대해서 알아본다.

2.2 공격 감지 방법

그림 1 과 같은 네트워크 환경에서 릴레이 노드가 외부로부터 공격을 받지 않고 신호 대 잡음비가 큰 채널을 가정하면 MP 복호기의 입력과 출력이 서로 다를 확률은 크지 않다. 이러한 채널에서 릴레이 노드에 공격이 가해져 정반대의 패러티 검사 비트를 전송하게 되면 복호기의 입력 부호가 반대가 된다. 하지만 반복적으로 복호화하는 과정에서 출력 부호는 원래의 부호를 갖게 된다. 따라서 MP 복호기의 에러를 바로 잡는 특성을 이용하여 일정 기간 동안 복호기의 입력과 출력의 부호가 서로 다른 노드들을 관찰함으로써 공격이 가해지는 릴레이 노드의 위치를 파악할 수 있다.

2.3 공격 보상 방법

외부로부터 공격을 받은 릴레이 노드의 위치가 2.2 의 방법을 통해 검출이 되면, 남아 있는 문제는 그러한 네트워크 환경을 개선하기 위해 보상 알고리즘을 구현하는 것이다. 본 논문에서는 오염된 릴레이로부터의 정보를 사용하지 않는 방법과 역으로 바꾸는 방법을 제안한다.

첫 번째 방법은, 액세스 노드에서 MP 복호화를 하는 과정에서, 오염된 릴레이 노드로부터 오는 정보를 이용하지 않는 방법이다. 오염된 정보를 이용하지 않음으로써 성능 저하가 예상되지만, 잘못된 정보를 사용하는 경우보다 더 나은 성능이 보장된다.

두 번째 방법은, 공격받은 릴레이의 위치와 정보를 정확하게 검출한다면 다시 역으로 정보를 바꾸는 방법이다.

Ⅲ. 컴퓨터 모의실험

컴퓨터 모의실험은 100 개의 소스 노드, 100 개의 릴레이 노드 환경에서 수행하였다. 모든 소스와 릴레이 노드들이 액세스 노드로부터 동일한 거리에 위치해 있다고 가정함으로써 채널 노이즈의 분산이 동일하다고 가정하였다. 공격 받는 릴레이의 위치를 찾아내기 위해 1000 개의 수신 샘플을 가지고 수행하였다.

그림 2 는 각각의 릴레이서 가해지는 공격이 항상 100%의 확률을 가지고 공격한다는 가정하에 BER 성능을 나타낸다. 전체 릴레이의 5%, 5 개의 릴레이가 공격을 당해도 성능이 크게 나빠지는 것을 볼 수 있고, 전체 릴레이의 15%, 15 개의 릴레이가 공격을 당하면 전체 네트워크가 동작을 안 한다고 볼 수 있다.

이러한 환경에서 2.2 절에 설명한 방법으로 릴레이 공격을 감지 했을 후, 2.3 절에 있는 보상 방법들을 사용했을 때의 성능을 나타낸다. 그림에서 볼 수 있듯이, 모든 보상 방법을 사용한 경우가 그렇지 않은 경우보다 항상 성능이 좋게 나오는 것을 확인할 수 있다. 또한 릴레이의 위치와 정보를 정확히 알 때, 오염된 릴레이로부터의 정보를 역으로 바꾸는 방법이, 그 정보를 사용하지 않는 경우보다 성능이 좋게 나오는 것을 확인할 수 있다.

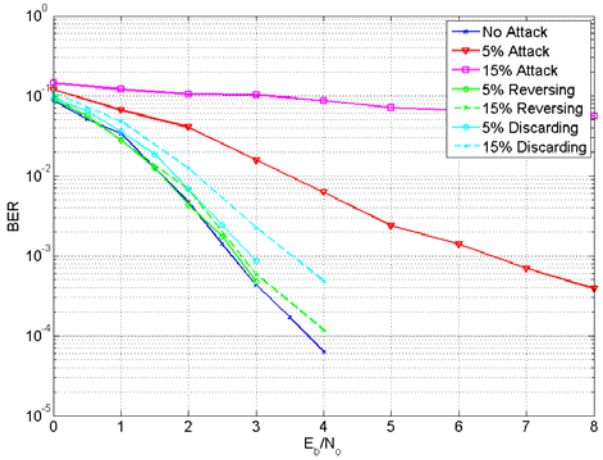

그림 2 WMA 네트워크 성능곡선

Ⅳ. 결론

본 논문에서는 협력적 네트워크 부호화를 사용하는 무선 네트워크 통신 환경에서 임의의 릴레이 노드들이 외부로부터 공격을 받아 잘못된 부호화 정보를 전송하는 경우, 액세스 노드에서 이러한 릴레이 노드들을 찾아내고 잘못된 정보를 복구하는 방법을 연구하였다.

ACKNOWLEDGMENT

이 논문은 2010 년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (중견연구자-핵심연구사업, N0. 2010-0026407)

이 논문은 2009 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 해외우수연구기관유치사업 연구임(K20902001632-10E0100-06010)

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.

[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.