DOI : 10.5392/JKCA.10.10.019

# Snoop 프로토콜의 보안상 취약점과 그 대책

## Security Vulnerability of Snoop Protocol and Its Countermeasure

**고윤미, 권경희**
단국대학교 전자계산학과 컴퓨터과학

Yun-Mi Go(alice8105@dankook.ac.kr), Kyung-Hee Kwon(khkwon@dankook.ac.kr)

**요약**

Snoop 프로토콜은 무선 네트워크에서 패킷 손실시 지역 재전송 기법을 이용하여 네트워크 성능을 향상시키지만 공격자에 의해 위조된 ACK 패킷 공격에는 어떠한 대응도 하지 못하는 보안상의 취약점을 갖고 있다. 따라서 본 논문에서는 이러한 문제점을 개선하기 위하여 버퍼를 추가한 Snoop을 제안한다. 제안된 Snoop은 위조된 ACK 패킷 공격에 의해 기존 Snoop 버퍼에 패킷이 저장되어있지 않더라도 추가 버퍼(extra buffer)에 저장된 패킷을 이용하여 지역 재전송이 이루어지게 한다. NS-2를 이용한 시뮬레이션 결과, 제안된 Snoop을 통해 위조된 ACK 패킷 공격을 대응할 수 있게 되어 더욱 안전한 Snoop 프로토콜을 구축할 수 있었다.

■ 중심어 : | Snoop | 무선 | 위조된 ACK 공격 |

**Abstract**

While Snoop improves network performance by using local retransmission in case of packet loss in wireless network, it has security vulnerability to be unable to countermeasure against falsified ACKs attacks. Therefore in this paper, we suggest a modified Snoop with an extra buffer in addition to original Snoop buffer. Even though packets are exhausted in original buffer by falsified ACKs attacks, proposed Snoop can locally retransmit the packets saved in the extra buffer. The simulation by NS-2 shows that proposed Snoop countermeasure efficiently against falsified ACKs attack and builds securer Snoop protocol.

■ keyword : | Snoop | Wireless | Falsified ACKs Attacks |

## I. 서 론

휴대전화나 노트북등의 이동기기의 보급이 활발해지면서 무선 인터넷의 수요가 급증하였다. 그러나 현재 유선망을 기준으로 설계된 인터넷 환경에선 무선 네트워크의 불안정한 링크에 의해 데이터가 손실된 것이 아니라 망에 의한 혼잡으로 간주한다. 그렇기 때문에 무선 네트워크에서 발생하는 통신 오류 및 핸드오프로 인한 패킷 손실에 대해 불필요한 혼잡제어 메커니즘을 호출하여 네트워크의 효율을 저하시키는 원인이 된다. 그러므로 유선과 무선구간내의 패킷 손실 원인이 다르기 때문에 손실 복구 메커니즘이 다르게 적용되어야 한다. 이러한 이유로 유무선 혼합망에 적합한 TCP로 수정되어지고 있으며 지금도 많은 연구가 진행되고 있다[1-8].

* 본 연구는 2009년 단국대학교 대학 연구비에 지원으로 연구되었습니다.

접수번호 : #100803-003
접수일자 : 2010년 08월 03일
심사완료일 : 2010년 10월 25일
교신저자 : 고윤미, e-mail : alice8105@dankook.ac.kr

특히 패킷 손실 시 재전송 메커니즘을 유선과 무선 구간에 따로 적용하면서 네트워크의 성능을 향상 시키는 방법으로 BS(Base Station: 기지국)에 Snoop 모듈 추가방법이 있다. Snoop 프로토콜은 무선구간에서 패킷 손실이 발생하면 FH(Fixed Host: 고정호스트)가 아닌 BS에서 재전송이 이루어진다. Snoop 모듈이 추가된 BS는 FH로부터 수신한 데이터를 버퍼에 저장 후 MH(Mobile Host : 이동호스트)로 전송하는데 무선구간에서 패킷이 손실되고 타임아웃이 발생하면 BS버퍼에 저장되어진 패킷을 재전송한다. Snoop은 무선 네트워크에서의 손실이 혼잡으로 인한 것인지 높은 에러율과 낮은 대역폭 등의 특징으로 인한 것인지를 구분하여 혼잡 제어 메커니즘을 호출한다. 그 결과 Snoop은 불필요한 혼잡제어 메커니즘 호출을 줄여 네트워크 성능을 향상시킨다.

무선 구간에서는 악의적인 공격자에 의해 스니핑과 침입 공격이 가능하다. 따라서 악의적인 공격자에 의해 MH와 같은 위조된 ACK 패킷을 생성하여 BS에게 전송하는 공격이 가능하게 된다. 악의적인 공격자에 의해 위조된 ACK 패킷을 생성하여 계속적으로 BS에게 전송하게 되면 버퍼에 저장되어 있는 패킷이 삭제되어 무선 구간의 패킷이 손실되어도 지역 재전송이 이루어지지 않는다. 그 결과 무선 구간의 패킷이 손실될 때 마다 FH에 혼잡 메커니즘이 호출되어 네트워크 성능이 저하 되게 된다. 따라서 본 논문에서는 이러한 문제점을 개선하기 위하여 BS의 Snoop 모듈에 버퍼를 추가하였다. BS는 위조된 ACK 패킷 공격을 탐지하면 제안하는 Snoop 프로토콜을 적용한다. 제안한 Snoop은 BS에서 ACK을 수신 하였을 경우 기존 버퍼에 패킷을 삭제하는 동시에 추가 버퍼(extra buffer)에 패킷을 저장한다. 이때 BS에 위조된 ACK 패킷 공격으로 인해 기존 버퍼에 패킷이 저장되어 있지 않고 무선 구간에서 패킷이 손실되었다면 제안한 Snoop은 추가 버퍼에 저장된 패킷을 이용하여 지역 재전송한다. 그 결과 위조된 ACK 패킷 공격시에 제안된 Snoop은 공격전의 기존 Snoop 성능과 유사함을 보였다. 이는 제안된 Snoop이 위조된 ACK 패킷 공격을 효과적으로 방어함을 의미한다.

본 논문의 구성은 다음과 같다. 2장에서는 유무선 환경에서 네트워크 성능향상을 위한 기법들을 분류한다. 또한 공격자에 의해 Snoop 프로토콜 공격이 이루어질 수 있음을 확인하고 이에 대한 대응방안에 대해서 살펴본다. 3장에서는 위조된 ACK 패킷 공격에 대응하기 위한 메커니즘을 제안한다. 4장에서는 제안한 메커니즘과 현제 메커니즘을 시뮬레이션을 통해 성능을 비교하였다. 마지막으로 5장에서는 결론 및 향후 과제에 대해서 살펴본다.

## II. 관련연구

Snoop은 무선 구간의 패킷 손실시 BS의 지역 재전송을 통해 네트워크 성능을 향상시키고 있다. 이와 관련해서 Snoop을 이용한 유무선 혼합망에서 패킷 손실 되었을 경우 혼잡 제어 메커니즘 호출을 최소화시키는 여러 기법들 제안되었다. 무선 네트워크의 연속적인 패킷 손실 시 BS의 버퍼 크기가 임계치 이상이 되면 FH에 Window- Size-Zero-ACK를 보내 빠른 복구를 하는 기법[5], BS가 MH로부터 ACK 패킷을 여러 개의 패킷으로 나누어서 FH에 전송하면 FH에서 윈도우의 크기를 빠르게 복구시키는 방법[6]이 있다. 또한 ACK 패킷에 무선 네트워크의 대역폭을 표시하는 플래그(flag)를 설정한다. 그 결과 송신측의 윈도우 사이즈를 zero으로 만들어 혼잡 메커니즘 호출을 방지하는 기법[7]이 있다.

이렇듯 많은 연구들이 효율적인 메커니즘과 재전송 알고리즘을 통해 성능 개선을 가져왔다. 하지만 공격자에 의해 Snoop 프로토콜이 정상적으로 빠른 패킷 복구를 하지 못하게 만드는 공격에 대해 대응하지 못하고 있다. 더욱이 기존에 Snoop은 위조된 ACK 에 의해 Snoop 버퍼에 저장되어 있는 패킷을 삭제하는 공격에 대한 대응 방법이 없다. 따라서 공격자에 의해 Snoop 프로토콜이 공격 시 공격을 탐지하고 대응하는 것이 시급하다. 본 연구에서는 위조된 ACK 패킷 공격에 대응하는 단순하면서도 효율적인 메커니즘을 제안한다.

## III. 제안하는 메커니즘

유선 네트워크 환경에서는 악의적인 공격자를 효율적으로 차단하고 관리하기 위하여 인증 및 보안관리 시스템을 적용하고 있다. 그러나 무선 네트워크 에서 인증을 통해 공격을 차단하는 방식은 너무 많은 오버헤드가 발생하여 효율적이지 못하다[9]. 본 논문에서는 Snoop 프로토콜에서 공격자에 의해 위조된 ACK 패킷 공격을 차단하기 위하여 기존의 인증방식이 아닌 다른 방안을 제시하고자 한다.

위조된 ACK 패킷 공격이란 악의를 가진 공격자가 정상적인 MH과 같은 위조된 ACK 패킷을 생성하여 계속적으로 BS에게 전송하는 기법이다. 위와 같은 공격 기법은 BS의 Snoop 버퍼에서 위조된 ACK 패킷에 대응하는 저장된 패킷을 삭제하게 만든다. 즉 정상적인 ACK 패킷과 위조된 ACK을 구별하지 못한 채 Snoop 버퍼에 저장된 패킷을 삭제하게 된다. 이때 무선 네트워크에서 위조된 ACK 패킷으로 인해 삭제된 패킷이 손실되었을 경우에 Snoop에서 지역 재전송이 이루어지지 않게 되고 MH에는 손실된 패킷을 전송받기 위하여 계속적으로 중복 ACK 패킷을 보내게 된다. 그 결과 FH는 혼잡으로 인한 패킷 손실로 간주하여 혼잡제어 메커니즘을 호출하게 된다. 즉 위조된 ACK 패킷 공격으로 인해 Snoop 프로토콜의 특징인 무선 네트워크에서 패킷이 손실시 지역 재전송 기법을 이용하여 전송률을 향상시키는 기능을 상실하게 만든다. 따라서 본 논문에서는 위조된 ACK 패킷 공격이 이루어지더라도 Snoop에서 지역 재전송이 이루어지게 하고자 한다.

이를 위해 BS의 Snoop 모듈에 버퍼를 추가하였다. 만약 BS에서 ACK 패킷을 받았을 경우 기존의 RTT/2 보다 짧은 시간의 ACK을 수신하거나 근거 없는 ACK 패킷을 받았을 경우 악의적인 공격자에 의해 위조된 ACK패킷 공격이 이루어지는 것으로 판단한다. 만약 위조된 ACK 패킷 공격이 이루어질 경우 기존 Snoop 프로토콜 방식에서 제안하는 Snoop프로토콜 방식이 적용되도록 설계하였다. 제안하는 Snoop 프로토콜은 ACK 패킷을 수신하게 되면 기존에 존재하는 버퍼에서 패킷을 삭제하는 동시에 추가 버퍼에 패킷을 저장한다. 만약 기존 버퍼에서는 삭제된 패킷이 손실로 인해 다시 재전송 되어야 할 경우에는 추가버퍼에서 저장된 패킷을 재전송하게 하여 Snoop 프로토콜의 효율성을 향상시킨다. 즉 제안한 Snoop에서는 BS에서 중복 ACK 을 수신 시 기존 버퍼에 패킷이 저장되어있으면 재전송이 이루어지고 그렇지 않을 경우에 다시 추가 버퍼에 패킷이 저장되어있는지 판단한다. 만약 추가 버퍼에 패킷이 저장되어있을 경우 지역 재전송을 한다.

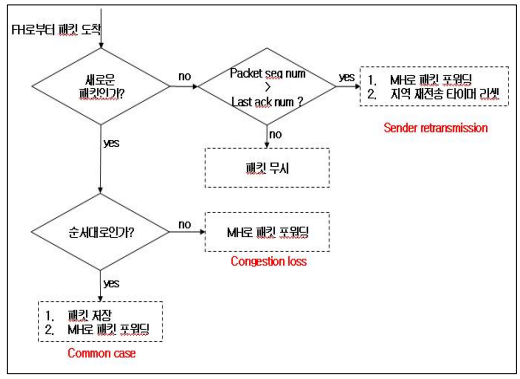


그림 1. 제안하는 Snoop 프로토콜의 snoop_data()

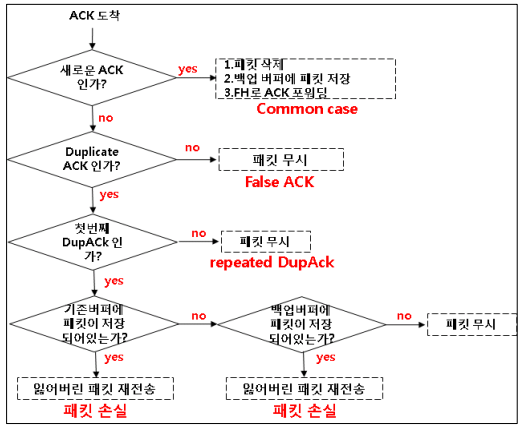


그림 2. 제안하는 Snoop 프로토콜의 snoop_ack()

[그림 1]은 제안하는Snoop프로토콜의 snoop_data() 프로시저로서 FH에서 전송된 패킷을 BS의 Snoop 모듈 버퍼에 저장하고 MH로 포워딩하는 역할이다. [그림 2]는 제안하는 Snoop 프로토콜의 snoop_ack() 프로시저로서 BS로 전송된 ACK 패킷에 의해 지역 재전송 여부를 판단한다. 이때 중복 ACK이오는 경우 기존 버퍼에 패킷이 저장되어있지 않다면 추가 버퍼에 패킷 존재

유무를 확인하여 재전송을 결정한다.

## Ⅳ. 시뮬레이션

### 1. 시뮬레이션 환경과 프로토콜

시뮬레이션은 네트워크 시뮬레이터인 NS-2[10]를 이용하였으며 다음과 같은 가정 하에 연구를 진행하였다.

첫째, TCP 타입은 TCP Reno 이다. 이는 TCP의 여러 가지 구현 중 대표적이며 가장 많이 이용되는 것이 Reno이기 때문이다. 둘째, 패킷 송수신 방법은 반이중(half-duplex) 으로 가정하였다. 셋째, 시뮬레이션 공간은 670 * 670 으로 전송 범위는 250m로 하였으며 MH의 개수는 3개로 랜덤하게 위치 시켰으며 트래픽은 TCP 사용하였다. 넷째, 시뮬레이션 중 하나의 MH 노드가 공격자임을 가정하고 있다. 이때 공격자 MH 노드는 계속적으로 위조된 ACK 패킷을 생성하여 BS에게 전송한다. 거리에 따른 신호 세기 감소는 Free space 모델과 Two-ray Ground 모델로 구성되었다. 물리계층의 802.11에서 전송방식은 DSSS(Direct Sequence Spread Spectrum)이며 채널 접근방식은 CSMA/CA를 사용한다. NS2에서 제공하는 에러모듈 중 ErrorModel/TwoStateMarcov 모듈을 802.11 표준 손실과정에 맞게 적용하여 시뮬레이션 하였다. [표 1]의 시뮬레이션과 관련된 파라미터는 NS-2에서 기본으로 설정된 것을 그대로 적용하였으며 시뮬레이션 시간은 100초간 지속된다.

[그림 3]은 시뮬레이션에 사용된 네트워크 모델이다. 8개의 노드가 위치해 있고 3번 노드는 트래픽을 발생시켜 전송하는 송신노드이다. 5번 노드는 BS노드로서 Snoop 모듈이 추가되어있다. 나머지 0.2.4번노드는 유선노드이고 6.7.8번 노드는 무선노드이다. 이때3번 노드에서 10초후 트래픽을 발생하여 각 무선 노드에게 전송한다. 8번 노드는 위조된 6번 노드의 ACK 패킷을 12초 이후부터 계속적으로 전송하는 공격자 노드이다. 즉 12초 이후에 8번 노드는 6번 MH의 ACK 패킷을 이용하여 위조된 ACK 패킷을 생성한다. 위조된 ACK 패킷은 5번BS 노드의 Snoop 모듈을 공격하여 무선 구간의 패킷 손실시 Snoop의 지역재전송이 일어나지 않게 하여 전송률을 향상시키는 기능을 상실하게 만들었다.

**표 1. 시뮬레이션 환경**

| 트래픽 타입 | | FTP(TCP) | |
|---|---|---|---|
| 물리 계층 | Propagation 모델 | Free space (r:거리) | $\frac{1}{r^2}$ (100m) |
| | | Two-ray Ground reflection | $\frac{1}{r^4}$ (250m) |
| | MAC | 802.11 DSSS (Direct Sequence Spread Spectrum) | |
| | 채널 접근방식 | CSMA/CA | |
| 에러율(PER) | | 0~10% | |
| 총 시뮬레이션 시간 | | 100s | |
| 토폴로지 | | 670 * 670 grid | |

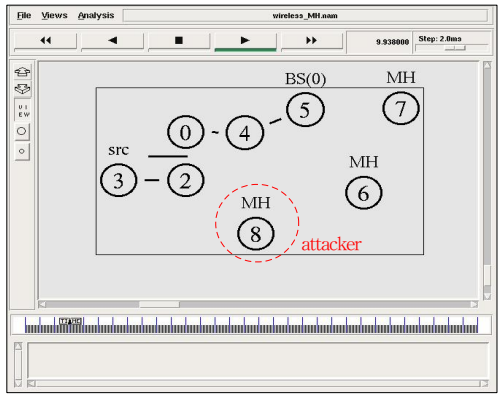


**그림 3. 네트워크 모델**

시뮬레이션은 두 가지 방법으로 진행하였다. 첫 번째 방법은 공격자 노드 8(MH 노드)번은 시뮬레이션 시작 후 5번 노드(BS 노드)로 6번 노드(MH노드) 와 같은 ACK 패킷을 위조하여 계속적으로 전송한다. 두 번째 방법은 첫 번째 방법에 무선구간의 에러율을 증가시키면서 실험하였다.

### 2. 시뮬레이션 결과

성능 평가는 위 두 가지 방법으로 시뮬레이션 하여 위조된 ACK 패킷 공격이 일어나기 전과 후의 Snoop 프로토콜의 혼잡 윈도우와 MH의 처리량을 확인하였

다. 또한 제안하는 메커니즘을 적용하였을 경우 위조된 ACK 패킷 공격시 혼잡 윈도우와 MH의 처리량을 확인하였다.

[그림 4]는 에러율이 1%일 때 TCP 혼잡 위도우 크기를 측정한 결과이다. 기존 Snoop 프로토콜은 위조된 ACK 패킷 공격이 이루어지게 되면 송신측의 중복 ACK 수신이 이루어져 혼잡 윈도우 크기가 감소된다. 즉 공격으로 인해 빈번히 혼잡 제어 메커니즘이 호출되어 혼잡 윈도우 크기가 감소되는 현상이 일어나게 된다. 따라서 기존 Snoop 프로토콜은 ACK 패킷 공격에 의해 불필요한 혼잡 제어 메커니즘을 빈번히 호출되어 네트워크 성능이 저하된다. 제안한 Snoop은 ACK 패킷 공격시 공격이 일어나지 않았을 때 Snoop의 혼잡위도우 크기 변화와 유사한 형태를 보이고 있다. 즉 위조된 ACK 패킷 공격에 의해 불필요한 혼잡 메커니즘이 호출되는 현상을 제거하게 되었다.

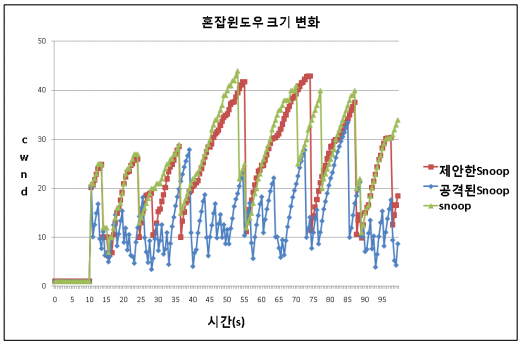


그림 4. 에러율이 1%일 경우 혼잡 위도우 크기

[그림 5]는 에러율이 3%일 때 TCP 혼잡 위도우 크기를 측정한 결과이다. 위조된 ACK 패킷 공격시 제안한 Snoop 프로토콜을 적용하였을 경우 기존의 Snoop 프로토콜에 비해 혼잡 윈도우 사이즈 변화량이 적게 되어 네트워크 성능이 좋은 것을 확인할 수 있었다. 더욱이 제안한 Snoop은 위조된 ACK 패킷 공격이 이루지지 않은 기존의 Snoop 프로토콜의 혼잡 윈도우 사이즈 크기가 유사한 형태로 변화하고 있다. 따라서 제안한 Snoop은 위조된 ACK 패킷 공격 방어하여 무선 구간의 패킷 손실시 지역 재전송으로 이루어져 네트워크 성능을 향상 시킨다.

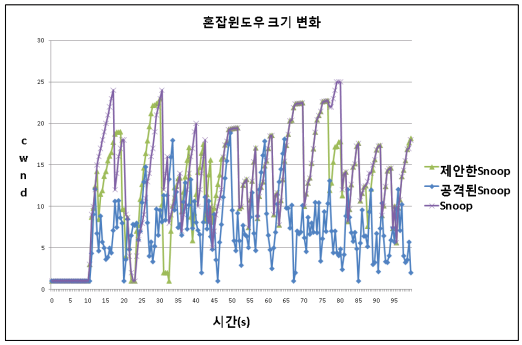


그림 5. 에러율이 3%일 경우 혼잡 위도우 크기

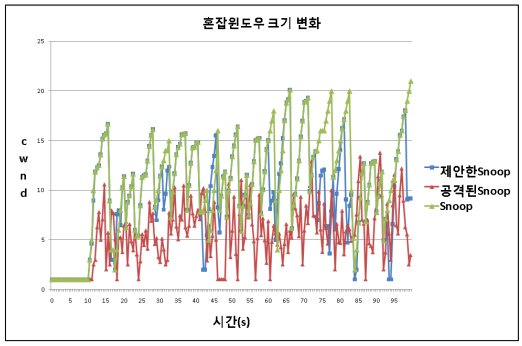


그림 6. 에러율이 5%일 경우 혼잡 위도우 크기

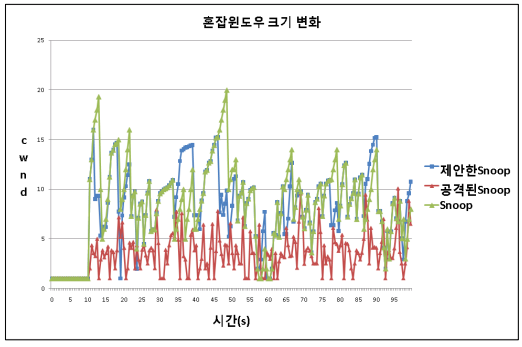


그림 7. 에러율이 10%일 경우 혼잡 위도우 크기

[그림 6]는 에러율이 5%일 때 TCP 혼잡 위도우 크기를 측정한 결과이다. [그림 7]는 에러율이 10%일 때 TCP 혼잡 위도우 크기를 측정한 결과이다. 기존 Snoop에서는 에러율이 높아짐에 따라 위조된 ACK 패킷 공격시 적은 혼잡 윈도우 사이즈가 유지되고 있음을 확인할 수 있다. 위조된 ACK 패킷 공격시 제안한 Snoop

프로토콜에서는 기존의 Snoop 프로토콜보다 혼잡 윈도우 사이즈가 크기 때문에 성능이 향상되었음을 보여준다. 또한 공격이 일어나지 않을 경우의 Snoop과 제안한 Snoop프로토콜의 혼잡위도우를 비교해본 결과 유사한 형태로 혼잡 윈도우가 변경되고 있음을 볼 수 있다. 즉 위조된 ACK 패킷 공격을 효과적으로 방어하고 있음을 확인할 수 있다.

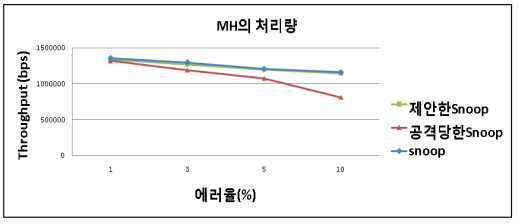


**그림 8. 에러율이 변화함에 따른 MH의 처리량**

그림 8은 기존 Snoop과 제안한 Snoop 알고리즘의 적용 여부에 따른 MH의 처리량을 측정한 결과이다. 위조된 ACK 패킷 공격 시 무선 구간의 에러율이 높아질수록 제안하는 Snoop 알고리즘을 적용하였을 경우와 적용하지 않았을 경우를 비교해본 결과 처리량의 이득이 커짐을 알 수 있다. 즉 기존 Snoop은 공격시 잦은 혼잡 제어 메커니즘의 호출로 인해 송신량이 줄어들 뿐만 아니라 불필요한 재전송이 일어나게 된다. 또한 공격이 일어나지 않을 경우의 Snoop 과 공격이 일어날시 제안한 Snoop을 적용했을 때 MH의 처리량을 비교해본 결과 유사함을 볼 수 있었다. 즉 제안한 Snoop에서는 공격이 이루어지더라도 무선 구간의 패킷 손실시 지역재전송을 통해 빠른 복구가 가능하게 하여 공격이 이루어지기 전의 MH 처리량과 유사함을 보이게 되었다.

## V. 결론

유무선 환경에서 성능향상을 위해 사용되는 Snoop은 악의적인 공격자에 의한 공격을 차단하고 대응하고 있지 않다. 더욱이 무선 네트워크에서는 전파가 도달 가능한 거리에 있는 MH은 패킷 스니핑이 가능하기 때문에 위조된 패킷을 쉽게 생성할 수 있게 된다. 따라서 Snoop의 효율성을 저해하는 위조된 ACK 패킷 공격이 가능하게 된다. 본 논문에서는 이러한 취약점을 보안하기 위하여 위조된 ACK 패킷 공격을 탐지 및 공격을 무효화 시키는 Snoop 프로토콜을 제안하였다. 제안하는 Snoop 프로토콜은 버퍼를 추가하여 위조된 ACK 패킷 공격에 대해 대응한다. 즉 공격이 이루어지고 있는 경우 BS에서 ACK 패킷을 송신하는 경우 기존 버퍼에서 패킷을 삭제하는 동시에 추가 버퍼에 패킷을 저장한다. 그 결과 무선 네트워크에서 패킷이 분실되어 BS에서 중복 ACK을 수신하였을 때 기존 버퍼에 패킷이 삭제되었다면 추가 버퍼에 저장된 패킷을 이용하여 재전송한다. 위조된 ACK 패킷 공격이 일어나지 않을 경우 기존 Snoop의 성능과 위조된 ACK 패킷 공격시 제안한 메커니즘의 성능의 유사함을 시뮬레이션을 통해 확인할 수 있었다. 따라서 제안한 Snoop은 위조된 ACK 패킷 공격을 효과적으로 대응할 수 있음을 확인하였다.

앞으로의 연구과제는 위조된 ACK 패킷 공격뿐만 아니라 다른 공격 기법에 대한 대응방안에 대해서 연구할 것이다.

## 참 고 문 헌

[1] 김진희, 권경희, “이동호스트의 수신신호를 이용한 유무선 혼합망에서의 TCP 성능향상”, 한국정보처리학회논문지C,제13-C권, 제5호, pp.635-640, 2006.

[2] 김진희, 권경희, “유·무선 혼합망에서 이동 호스트의 패킷 손실 예측을 통한 TCP 성능향상”, 한국콘텐츠학회논문지, 제7권, 제1호, pp131-138, 2007.

[3] 김윤주, 이미정, 안재영, “무선망에서의 TCP성능향상을 위한 제한적인 Indirect-ACK", 정보과학회 논문지 I, Vol.30, No.2, pp.233-243, 2003.

[4] 문영성, 강인석, “개선된 Snoop 기법을 이용한 무선 TCP 성능향상 방안”, 한국정보과학회 논문지 I, Vol.32, No.1, pp12-19, 2005.

[5] 김용, 성호철, 현호재, 한선영,“ Snoop 프로토콜에

서 혼잡제어 지연을 통한 이동망상에서의 TCP 성능향상 기법", 한국정보처리학회논문지 C, Vol.8, No.3, pp.351-358, 2001.

[6] 진교홍, "유무선 복합망에서 Acknowledgement 패킷의 분할을 통한 TCP 프로토콜의 성능 향상 기법", 한국정보처리학회논문지 C, Vol9-C, No.1, pp.39-44, 2002.

[7] S. J. Seok, S. B. Hoo, and C. H. kang, "A-TCP: A Mechanism for Improving TCP Performance in Wireless Environments," in Proc. of IEEE Broadband Wireless Summit, 2001.

[8] Fang Liu, Wen-bo, and Yuan-an Liu, "A New S cheme Improve TCP over Wireless Networks," WCNC 2004/IEEE, Vol.3 pp.1506-1509, 2004.

[9] 고윤미, 권경희, "IEEE 802.11에서의 복제된 AP 탐지 및 차단 기법", 한국콘텐츠학회논문지, 제10권, 제5호, pp.45-51, 2010.

[10] http://www.isi.edu/nsman/ns

## 저 자 소 개

**고 윤 미 (Yun-Mi Go)** 정회원

- 2004년 : 단국대학교 전자계산학과(이학사)
- 2007년 : 단국대학교 전자계산학과 컴퓨터과학(이학석사)
- 2008년 ~ 현재 : 단국대학교 전자계산학과 컴퓨터과학(박사과정)

<관심분야> : 무선 네트워크, 이동통신

**권 경 희(Kyung-Hee Kwon)** 정회원

- 1976년 : 고려대학교 물리학과(이학사)
- 1986년 : Old Dominion Univ. Dept. of Computer Scince (M.S.)
- 1992년 : Louisiana State Univ. Dept. of Computer Science(Ph.D.)
- 1979년 ~ 1984년 : 산업연구원 연구원
- 1993년 ~ 현재 : 단국대학교 교수

<관심분야> : 컴퓨터 네트워크, 알고리즘 분석 및 설계, 웹 공학