

무선 저전력 통신을 위한 Sleep 모드의 세분화된 재정의

김구원^o 박창윤

중앙대학교 컴퓨터공학부

antonio91@cnlab.cse.cau.ac.kr cypark@cau.ac.kr

Redefining the Sleep-mode Operation For Wireless Low-power Communication

GuWon Kim^o ChangYun Park

Dept. of Computer Science & Engineering, Chungang Univ.

요 약

이동 단말기 또는 센서 등이 사용하는 무선 통신에서는 통신에 소모되는 전력을 줄이는 문제가 중요시 된다. 따라서 802.11 무선 LAN의 PSM과 같이, 대부분의 무선 통신 기술들은 일시적으로 NIC를 꺼서 전력소모를 줄이는 Sleep 모드 기능을 제공하고 있다. 그러나 Sleep 기간 동안 해당 단말로 보내져야 할 트래픽이 다양한 형태로 발생할 수 있다는 점을 깊이 고려하지 않고 Sleep 모드의 동작을 정의하였으며, 그 결과 예상하지 못한 현상이 발생할 가능성이 상존한다. 본 연구에서는 이와 같은 현상의 예로서, 802.11의 PSM 노드에 발생할 수 있는 성능 반전과 에너지 소모를 통한 서비스 거부 공격을 제시한다. 또한 이와 같은 비정상적인 현상을 방지하는 방법으로서 기존의 Sleep을 폐쇄적(Closed) Sleep과 개방적(Open) Sleep으로 세분화할 것을 제안한다.

1. 서 론

모바일 기기의 사용 급증으로 무선통신은 이제 대부분의 통신 가능한 기기에 필수 요소로 자리 잡고 있다. 무선통신을 사용하는 대부분의 기기는 한정된 전력으로 운용되며 특히 센서와 같은 경우 초기 설치 이후 전력을 보충할 수 없는 경우도 있다. 이런 이유로 무선통신에서의 전력 소모 문제는 중요한 과제가 되었다. 이를 해결하기 위해 대부분의 무선통신 기술들은 전력 절약에 대한 해결책을 가지고 있다. 장자는 것과 같이 일시적으로 NIC의 기능을 중지하여 데이터가 전송되지 않을 때는 기기의 소비 전력을 최소화하는 Sleep 방식이 그것이다.

하지만 기기는 sleep 상태에서 계속해서 네트워크에 연결된 채로 필요한 작업을 수행한다. 이 때 Sleep 모드의 기기에는 다양한 트래픽이 발생할 수 있고 이는 예상치 못한 결과를 가져올 수 있다. 본 연구에서는 802.11 무선 LAN에 초점을 맞추어 이와 같은 현상의 예로 성능 반전과 에너지 소모를 통한 서비스 거부 공격을 제시한다. 또한 이런 현상을 방지하기 위해 Sleep 모드를 폐쇄적(Closed) Sleep 모드와 개방적(Open) Sleep 모드로 세분화할 것을 제안한다.

2. 관련 연구

2.1 802.11 무선 LAN의 PSM

무선 인터넷의 표준으로 IEEE에서 발표한 802.11은 PSM(Power Save Mode)을 사용하여 전력을 절약한다. PSM에 들어가는 노드는 AP에게 자신이 PSM에 들어감을 알리고 PSM에 들어간 후로는 주기적으로 깨어나 AP의 beacon frame을 받는다. Beacon frame에는 TIM(Traffic Indication Map)이 있어 노드에게 전달되어야 할 버퍼링된 메시지가 있는지를 알려준다. 만약 버퍼

링된 메시지가 있다면 노드는 AP에게 PS-Poll frame을 보내고 AP로부터 버퍼링된 프레임의 받는다. 만약 받아야 할 버퍼링된 데이터가 더 있을 경우 AP는 노드로 보내는 데이터의 More Data Bit를 1로 세팅한다. AP는 다시 PS-Poll을 보내 More Data Bit가 0이 될 때까지 데이터를 받는다[1].

CISCO에서는 PSM을 두 가지로 나눠 Fast PSP와 Max PSP로 구분하였다. Max PSP는 802.11 표준의 PSM과 동일하다. Fast PSP는 속도 향상을 위해 802.11 표준을 수정한 것으로서 PSM 노드가 많은 양의 데이터를 전송해야 될 때 일반모드인 CAM(Constant Access Mode)으로 전환하고 전송이 끝난 후에는 다시 PSM으로 돌아간다[2].

2.2 Zigbee의 Sleep 모드.

센서네트워크에서 주로 사용되는 Zigbee는 중앙에 네트워크를 관리하는 관리자를 둔다. 각각의 노드는 오랫동안 데이터를 송수신하지 않을 경우 관리자에 의해서 또는 자신의 의지로 sleep 상태에 들어갈 수 있다. Sleep 상태에서는 데이터를 전송하지 않으며 sleep 상태의 노드에게 데이터를 전송하기 위해 polling 방식을 사용한다. 만약 A라는 노드가 sleep 상태의 B라는 노드에게 데이터를 보내려 한다면 A 노드는 데이터를 관리자에게 전송하고 관리자는 B 노드에게 전송될 데이터가 있다는 내용의 beacon을 방송한다. 이 방송을 들은 B 노드는 관리자에게 데이터를 요구하고 관리자는 데이터를 전송하게 된다. 이때 관리자는 각각의 sleep 상태의 노드에 대한 버퍼를 두어야 한다[3].

2.3 Bluetooth의 Sniff, Hold, Park 모드

Bluetooth는 기본적으로 Piconet을 관리하는 master와 master와 연결되는 slave로 구성되며 전력을 절약하기 위해 노드의 상태를 Sniff, Hold, Park의 세가지 모드로 나누었다. Sniff 모드는 slave만이 될 수 있다. 일반모드에서는 slave가 각각의 master-to-slave 슬롯마다 master로부터 데이터를 수신한다. 하지만 Sniff 모드에서는 매 슬롯마다 데이터를 수신하지 않고 Sniff Interval만큼의 슬롯을 건너뛰어 데이터를 수신한다. slave는 메시지를 받지 않는 동안에 sleep할 수 있다. Hold 모드에서는 데이터의 전송이 필요 없을 때 slave가 master에 의해서 또는 자신의 의지로 일정기간동안 sleep하게 된다. 이때 slave는 채널에는 연결되어 있으나 일정기간이 끝나기 전에는 데이터를 수신할 수도, 깨어날 수도 없다. 마지막으로 Park 모드는 채널의 연결을 끊고 MAC 주소 또한 갖지 않으나 master와의 동기화를 위한 정보나 방송 메시지는 듣는다[4]. 위의 내용을 종합하면 sleep기간 중 수신되는 데이터를 받는 것은 Sniff 모드뿐임을 알 수 있다.

3. 802.11 Sleep모드에서 발생할 수 있는 예상 외 현상

802.11의 Sleep 모드의 동작을 보면, sleep 중에 도착하는 트래픽을 sleep에서 깨어난 후 polling으로 가져오도록 되어 있다. 즉, sleep 기간 중에 노드로 전송되는 트래픽을 어떻게 처리할 것인지에 대해 사용자가 선택할 수 있는 방법이 없다. 따라서 Sleep 모드의 노드로 수신되는 데이터의 유형에 따라 예상치 못한 현상이 발생할 수 있다.

3.1 Busy PSM 노드에 의한 성능 반전

802.11의 PSM 노드는 전력 절감을 위해 sleep 상태를 유지하지만 주기적으로 sleep 상태를 벗어나 AP와 통신하게 된다. 이 때 같은 AP와 통신하는 일반모드의 다른 노드들은 PSM 노드에 의해 성능이 저하되지는 않는다는 것이 일반적인 예상일 것이다.

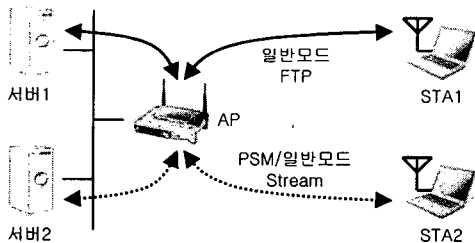


그림 1 PSM 노드로 인한 성능 반전

그림 1에서 STA1과 STA2는 같은 AP에 연결되어 있으며 STA1은 일반모드이고 STA2는 PSM이다. STA1이 서버1과 통신하고 있다고 가정하자. STA2가 sleep 상태이면 STA1은 보다 많은 대역폭을 사용할 수 있어야 한

다. 그러나 STA2가 서버2로부터 MPEG과 같은 스트리밍 데이터를 수신하는 경우, STA2는 polling을 통한 데이터 수신을 빈번히 수행하여야 하며, 이로 인해 STA1이 사용할 수 있는 대역폭이 줄게 되어 성능 반전이 일어날 수 있다. 즉, 어떤 노드가 PSM으로 동작하면 이웃노드에게 성능 감소를 일으키는 현상이 발생하는 것이다[5]. 이런 현상이 발생하는 이유는 수신되기 위해 대기 중인 데이터가 많아질 수 있다는 점을 간과하고 polling보다 효율적인 방법을 고려하지 않았기 때문이다.

3.2 에너지 소모를 통한 서비스 거부 공격

서비스 거부(DoS) 공격이란 사용자의 네트워크 기능이 일시적으로 제 기능을 발휘하지 못하거나 프로그램 또는 파일을 못 쓰게 되는 상황을 가리킨다. 여러 가지 공격 방법이 있으며 대표적으로 데이터 버퍼 용량보다 더 많은 량의 트래픽을 보내는 버퍼 오버플로우 공격이 있다. 전력 공급이 한정된 센서와 같은 기기의 경우 불필요한 수신에 따른 전력 소모는 기기의 수명을 단축시켜 서비스가 중단될 수 있다. 따라서 제한된 전원을 갖고 있는 기기에게 의도적으로 과도한 트래픽을 보내게 되면 서비스 거부 공격과 유사한 효과를 나타내게 된다. 본 연구에서는 이를 에너지 소모를 통한 서비스 거부 공격이라 부른다.

현재의 802.11 표준과 같이 PSM 노드가 sleep에서 깨어난 후 데이터를 무조건 수신한다면 위와 같은 상황에서 PSM 노드는 불필요한 데이터를 대량으로 수신하게 된다. 이는 곧 에너지 소모를 통한 서비스 거부 공격에 노출되었다고 볼 수 있으므로 전력 소모를 줄이기 위해 sleep을 한 효과가 없어지게 된다. 즉, sleep 기간 동안 전달되는 데이터에 대해 관심이 없는 PSM 노드라 하더라도 서비스 거부 공격에 의해 데이터를 수신해야만 하고, 결국 PSM 노드는 많은 양의 전력을 소비하게 되는 것이다. 이런 현상이 발생하는 이유는 PSM 노드의 성격을 한정지어 sleep 기간 중 수신되는 데이터를 받을 수밖에 없게 되어있기 때문이다.

4. Sleep 모드 동작의 재정의 및 효과

4.1 Sleep 모드 동작의 세분화된 재정의

PSM 노드가 Sleep 기간 중 수신되는 데이터를 처리하는 규칙을 하나로 제한하였기 때문에 위와 같은 문제가 발생한다. 이 문제를 해결하기 위해 Sleep 모드를 개방적(Open) Sleep과 폐쇄적(Closed) Sleep이라는 두 가지로 나누는 것을 제안한다.

개방적 Sleep 모드란 통신을 계속할 의사는 있지만 전력 절약을 위해 sleep하는 것을 말하며, sleep 기간 동안 수신하지 못한 데이터는 sleep에서 깨어난 후 받도록 한다. 802.11의 PSM이 이에 해당한다. 반대로 폐쇄적 Sleep 모드란 sleep 기간 동안 도착하는 데이터를 sleep에서 깨어난 후 받을 필요가 없다. Bluetooth의 Hold 모드가 이와 유사한 개념이다.

개방적 Sleep 모드의 경우는 sleep 기간 동안 전달되

지 못한 트래픽을 효율적으로 처리하는 기법이 수반되어야 한다. 802.11의 AP와 같은 중계 기기에서는 데이터를 임시적으로 저장할 버퍼가 충분히 준비되어야 하며, sleep에서 깨어났을 때 이를 빠르게 전송할 수 있어야 한다. 802.11의 PSM이 의미적으로는 개방적 sleep에 해당되지만, 버퍼에 저장된 데이터를 프레임 단위로 polling을 해서 수신하므로 효율적인 동작면에서는 개방적 sleep으로서 부족하다고 할 수 있다. Cisco에서 제안한 Fast PSP는 이러한 문제점을 개선하기 위해 버퍼에 있는 트래픽을 처리할 때까지 Sleep 모드에서 잠시 벗어나는 기법으로서 개방적 sleep에 보다 적합하다고 할 수 있다.

폐쇄적 Sleep의 경우는 sleep 기간 동안 전달되는 데이터에 대해서는 관심이 없는 모드이다. 따라서 중간 노드에서의 버퍼링이나 깨어난 후의 수신 동작은 고려할 필요가 없다. 대신에 sleep과 교차하는 awake 상태에서 송수신을 원활히 할 수 있는 기법이 마련되어야 한다.

4.2 모드 선택 및 효과

Sleep 모드의 선택은 노드의 전력 상황과 노드의 통신 패턴에 따라 선택될 수 있다. 일반 사용자가 사용하는 노트북 또는 PDA 노드의 경우에는 전력 절약을 위해 sleep을 한다고 하더라도 양방향 데이터 전송이 언제라도 일어나는 Busy Sleep 노드에 가깝다고 할 수 있다. 이 경우는 미사용 시간 동안의 전력 절감은 물론, 효율적이고 원활한 수신이 지원되어야 하므로 개방형 Sleep 모드가 적합한 선택이라고 할 수 있다.

802.11 PSM은 AP에 버퍼링된 데이터를 수신하는 작업이 비효율적이므로 앞에서 설명한 성능 역전 현상이 발생한다. Sleep 동작을 개방형과 폐쇄형으로 세분화해서 정의한다면, 프레임 하나씩을 polling을 하는 현재의 동작을 각각의 특성에 맞추어 수정할 수 있을 것이다. 예를 들어, 개방형 Sleep 노드의 경우에는, 그림2에 나타난 바와 같이, 한번의 polling을 버퍼에 있는 모든 프레임에 대해 수신 요청으로 해석하도록 확장한다면 Busy Sleep 노드에 의한 성능 반전을 방지할 수 있을 것으로 예상된다.

센서 노드와 같이 전력 소비에 매우 민감하면서 일정한 주기로 단방향 송신을 주로 하는 경우에는 폐쇄형 Sleep이 적합하다고 할 수 있다. 이 경우에 개방형 Sleep을 적용한다면 노드 자신이 필요로 하지 않는 데이터 수신 때문에 전력 소비가 높아질 수 있다. 또한 폐쇄형 Sleep을 선택한다면 에너지 소모를 통한 서비스 거부 공격도 사전에 방지하는 효과를 얻을 수 있을 것이다.

5. 결론

802.11 무선 LAN에서 PSM은 노드의 전력 소비를 줄이기 위해서 사용된다. 그러나 sleep 기간 동안 PSM 노드로 수신되는 트래픽이 다양하여 이에 따른 예상치 못한 현상이 발생할 수 있다. 본 연구에서는 이러한 예외 스트리밍 데이터를 수신할 때에 일반모드로 동작하는 것보다 PSM으로 동작하는 것이 오히려 다른 노드에게 피해를 주는 성능 반전과, 전력 절약을 위해 PSM으로 동작하는 노드에게 과도한 트래픽을 발생시켜서 에너지 소모를 통한 서비스 거부 공격을 하는 것이 가능하다는 점을 제시하였다.

이와 같은 문제는 sleep 기간 중 수신되는 데이터를 하나의 규칙으로만 처리하였기 때문에 발생하며, 이에 따라 Sleep 모드를 폐쇄적 Sleep 모드와 개방적 Sleep 모드로 구분할 것을 제안하였다. 개방적 Sleep 모드는 PSM 노드가 적극적으로 데이터를 수신하여 스트리밍 데이터 수신으로 인한 성능 반전 현상을 방지할 수 있고, 폐쇄적 Sleep 모드는 sleep에서 깨어난 후에도 버퍼링된 데이터를 수신하지 않아 서비스 거부 공격을 방지할 수 있다. 즉, PSM 노드가 sleep 상태에서 수신되는 데이터의 성격에 따라 능동적으로 대처하여 전송 효율과 전력 소비 효율도 높일 수 있는 효과를 가져 올 수 있다. 향후 연구로는 폐쇄형 Sleep 모드와 개방형 Sleep 모드를 구체적으로 정의하고 실제 PSM 노드에 적용할 수 있도록 구현하는 과정이 필요할 것이다.

6. 참고문헌

[1] IEEE 802.11 Standard, "Part11: Wireless LAN Medium Access(MAC) and Physical Layer(PHY) Specifications", IEEE Computer Society
 [2] http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_chapter09186a00801f0db1.html
 [3] IEEE 802.15.4 Standard, "Part15.4: Wireless Medium Access(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Computer Society
 [4] Bluetooth SIG, Inc., "Specification of the Bluetooth System", <http://www.bluetooth.org>
 [5] Do Han Kwon, Sung Soo Kim, Chang Yun Park and Chung Il Jung, "Experiments on the Energy Saving and Performance Effects of IEEE 802.11 Power Saving Mode (PSM)", *Proceeding of ICOIN 2005*, Jeju Island, Korea, January/February 2005

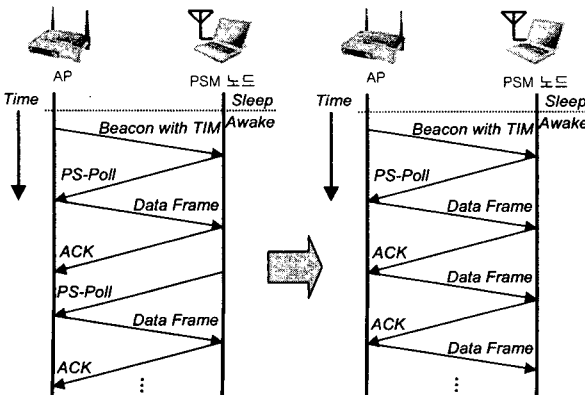


그림 2 PSM의 polling 방식 개선