韓國컴퓨터情報學會 論文誌
第14卷 第10號, 2009. 10.

2009-14-10-3-1

안전한 6LoWPAN 단편화 패킷 재전송 기법에 관한 연구

김 현 곤*

A Secure 6LoWPAN Re-transmission Mechanism for Packet Fragmentation against Replay Attacks

hyungon Kim*

요 약

6LoWPAN은 IEEE 802.15.4 MAC과 PHY 계층 위에서 IPv6 패킷을 전송하기 위해 IPv6 헤더 압축, TCP/UDP/ICMP 헤더 압축, 단편화 및 재조립 등을 수행하는 적응계층이다. 그러나 보안 관점에서 보면 기존 IP 계층에서 단편화 및 재조립으로 인한 보안 취약점을 그대로 가지고 있으며 6LoWPAN 적응계층 고유의 새로운 보안 취약점에 노출될 수 있다. 센서 노드는 특성상 재생공격으로 인해 단편화된 패킷의 재전송이 빈번하게 발생하게 되면 심각한 통신장애가 발생한다. 본 논문에서는 6LoWPAN 계층에서 패킷 단편화로 발생할 수 있는 보안 취약점을 분석하고 재생공격으로 인한 재전송을 최소화할 수 있는 메커니즘을 제안하였다. 6LoWPAN 표준을 기반으로 추가적인 재전송 절차 및 단편화 패킷 구조를 설계하고 재전송 지연시간을 분석하였다. 제안하는 메커니즘은 타임스탬프, 난스, 체크섬을 도입하여 센서 노드에 가해질 수 있는 재생공격을 최소화한다. 이를 통해 불필요한 패킷 단편화 및 재조립을 제거함으로써 센서 노드의 재조합 버퍼 오버플로우, 통신 속도 저하, 컴퓨팅 자원 손실, 노드 재부팅 등을 최소화시켜 통신의 신뢰도를 높일 수 있다.

Abstract

The 6LoWPAN(IPv6 Low-power Wireless Personal Area Network) performs IPv6 header compression, TCP/UDP/ICMP header compression, packet fragmentation and re-assemble to transmit IPv6 packet over IEEE 802.15.4 MAC/PHY. However, from the point of view of security, It has the existing security threats issued by IP packet fragmenting and reassembling, and new security threats issued by 6LoWPAN packet fragmenting and reassembling would be introduced additionally. If fragmented packets are retransmitted by replay attacks frequently, sensor nodes will be confronted with the communication disruption. This paper analysis security threats introduced by 6LoWPAN fragmenting and reassembling, and proposes a re-transmission mechanism that could minimize re-transmission to be issued by replay attacks. Re-transmission procedure and fragmented packet structure based on the 6LoWPAN standard(RFC4944) are designed. We estimate also re-transmission

• 제1저자 : 김현곤
• 투고일 : 2009. 07. 30, 심사일 : 2009. 09. 22, 게재확정일 : 2009. 10. 26.
* 목포대학교 정보보호학과 교수

delay of the proposed mechanism. The mechanism utilizes timestamp, nonce, and checksum to protect replay attacks. It could minimize reassemble buffer overflow, waste of computing resource, node rebooting etc., by removing packet fragmentation and reassemble unnecessary.

▸ Keyword : 6LoWPAN, 단편화(Fragmentation), 재전송(Re-transmission), 보안(Security), 난스(nonce)

Ⅰ. 서 론

6LoWPAN(IPv6 over Low power Wireless Personal Area Network)[1~2]은 IP를 사용함으로써 기존에 구축된 통신 및 응용서비스 인프라를 그대로 이용할 수 있어서 비용이 절감될 뿐만 아니라 잘 알려지고 검증된 IP 기술들을 사용할 수 있어서 신뢰성과 안정성을 도모할 수 있다. 그리고 LoWPAN에서는 기존 네트워크들에 비해 상당히 많은 수의 센서 노드가 배치되어야 하므로 큰 주소공간과 자동 주소설정과 같은 기능을 내장하고 있는 IPv6가 적합하다. 센서 네트워크에 IPv6 기술을 접목하기 위한 표준화는 IETF의 6LoWPAN 워킹그룹에서 추진하고 있다. 계층 2에 IEEE 802.15.4[3~4]를 기반으로 하는 센서 네트워크에 IPv6를 지원하며, 통신 환경으로서는 저전력, 20~250Kbps의 데이터 전송률, 900~2400MHz의 주파수 대역에서 최소형 메모리와 최소형 프로세서만을 장착한 센서 응용을 대상으로 한다. 따라서 열악한 통신환경을 고려하여 어떻게 하면 데이터 전송속도가 느린 IEEE 802.15.4 기술을 통해 사이즈가 큰 IPv6 패킷을 효율적으로 그리고 안전하게 전달할 것인지가 주요한 이슈 중에 하나이다. 이를 위해 6LoWPAN 적응계층에서는 단편화(fragmentation)와 재조립(re-assemble), IPv6 헤더 압축, TCP/UDP/ICMP 헤더 압축 등의 기능들을 정의하고 있다.

그러나 현재의 6LoWPAN 적응계층 표준[1]에 의하면 보안에 대한 고려가 미흡하며 센서 네트워크에서 발생할 수 있는 재밍과 같은 물리적인 공격, 웜홀 공격, 블랙홀 공격 등에 대한 취약점만이 분석되어 있다[5~6]. 따라서 여러 측면의 보안 위협성(security threats)과 다양한 공격 시나리오들이 분석되어야 하고 이를 기반으로 취약점들을 제거할 수 있는 보안 기술들이 정의되어야 한다. 특히, 6LoWPAN 적응계층의 특성상 초경량(light-weight)이고 추가적인 컴퓨팅 자원, 메모리 자원, 센서 노드의 가격을 최소화할 수 있는 방안이 고려되어야 한다.

본 논문에서는 6LoWPAN 적응계층에서 단편화와 재조립으로 인해 발생할 수 있는 보안 취약점을 분석한다. 그리고 이를 기반으로 패킷 신선도 유지와 재생공격을 막고 패킷 재전송으로 인한 수신측 노드의 재조합 버퍼 오버플로우, 통신 속도 저하, 컴퓨팅 자원 손실, 노드 정지 등의 취약성을 최소화 할 수 있는 재전송 메커니즘을 설계하고자 한다.

본 논문의 구성은 제 1장의 서론에 이어, 제 2장에서는 관련 연구로서 6LoWPAN에서의 단편화와 재조립 기법을 알아보고, 제 3장에서는 패킷 단편화를 이용한 기존의 공격들을 조사하고, 6LoWPAN 적응계층에서 노출될 수 있는 보안 위협성을 분석하였다. 이를 기반으로 제 4장에서는 본 논문에서 제안하는 패킷 재전송 절차와 단편화 패킷 구조를 기술하였다. 제 5장에서 메커니즘의 성능분석 결과를 기술하고 마지막으로 제 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 센서 네트워크의 TCP 패킷 재전송 기법

센서 노드는 노드 자체의 컴퓨팅 능력이나 통신환경이 매우 제한적이기 때문에 이를 고려한 재전송 기법들에 대한 연구가 활발히 전개되고 있다. 특히, 센서 네트워크에서 TCP 계층에서의 혼잡(congestion)에 의해 발생하는 패킷 재전송을 최소화할 수 있는 다양한 기법들이 제안되고 있다. DTC(Distributed TCP Cashing)[7] 기법은 링크계층과 연동되어 지역 재전송과 세그먼트 저장 방법을 이용한다. 종단간 재전송을 회피하고, 각 노드들이 TCP 세그먼트를 캐싱하고, 손실 발생 시 캐싱된 데이터로 지역 재전송을 하여 손실을 최소화시킨다. ESRT(Event to Sink Reliable Transport)[8]는 신뢰성 있는 센서 데이터 전송을 위해 싱크 노드가 소스 노드에게 상태 보고서를 전송하고 이를 기반으로 관측과 혼잡제어를 수행한다. CODA(Congestion Detection and Avoidance in Sensor Network)[9]는 채널 모니터링과 수신측 버퍼 사용량을 기준으로 혼잡을 감지하고, 혼잡 감지 시 송신지에 backpressure 신호를 전송하여 재전송을 최소화한다.

2.2 6LoWPAN 적응계층 개요

6LoWPAN 적응계층은 그림 1과 같이 상위의 네트워크 계층인 IPv6와 하위의 IEEE 802.15.4 MAC/PHY 계층 사이에 위치하여 기존의 두 프로토콜을 변형시키지 않고 그대로 접목되도록 중간에 가교 역할을 수행한다. IPv6 패킷의

MTU(Maximum Transmission Unit) 크기는 1280 바이트이고, IEEE 802.15.4의 PPDU(Physical Protocol Data Unit)는 127바이트이므로 IEEE 802.15.4 프레임은 IPv6의 MTU를 그대로 탑재할 수 없다.

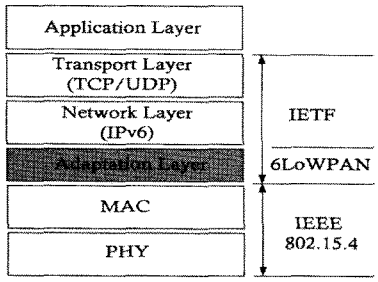

그림 1. 6LoWPAN 적응계층
Fig. 1. 6LoWPAN Adaptation Layer

또한 MAC 프레임 오버헤드가 25바이트를 차지하고, MAC 계층 의 보안을 위해 최대 오버헤드를 차지하는 AES-CCM-128을 사용할 경우, 21바이트가 추가된다. 참고로 AES-CCM-32 또는 AES-CCM-64의 경우, 각각 9 또는 13 바이트가 추가된다. 이로 인해 IP 계층에서 사용할 수 있는 용량은 81바이트가 된다. 따라서 IPv6 패킷이 81바이트를 넘는 경우에는 패킷 단편화가 이루어져야만 IEEE 802.15.4 프레임에 탑재할 수 있다. 한편, IPv6 프로토콜은 기본적으로 중간 노드에서 패킷 단편화를 지원하지 않는다. 이를 위해 패킷 단편화 기능을 수행해주는 6LoWPAN 적응계층이 필요하게 되었다. 6LoWPAN 패킷 단축기법을 그림 2에 나타내었다[1]. 6LoWPAN에서는 dispatch를 사용하여 일반적인 IPv6 패킷인지, 6LoWPAN 패킷인지, IPv6 헤더가 압축되는지, 메쉬 라우팅인지, 패킷이 단편화되어져야 하는지를 표현한다. 여기서 dispatch 헤더 패턴은 표1과 같다.

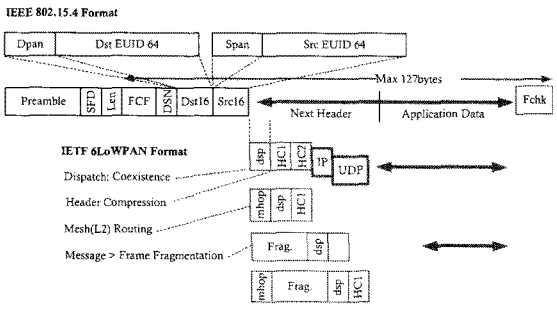

그림 2. 6LoWPAN 패킷 압축
Fig. 2. Compression of 6LoWPAN Packet

표 1. 디스패치 헤더 패턴
Table 1. Dispatch Header Pattern

패턴	패턴 이름	의미
00xxxxxx	NLAP	Not a LoWPAN Frame
01000001	IPv6	Uncompressed IPv6 Address
01000010	LOWPAN_HC1	LOWPAN_HC1 Compressed IPv6
01010000	LOWPAN_BC0	LOWPAN_BC0 Broadcast
10xxxxxx	MESH	Mesh Header
11000xxx	FRAG1	Fragmentation Header(first)
11100xxx	FRAGN	Fragmentation Header(subsequent)

IPv6의 헤더 필드에 대한 압축은 다음과 같다. "Version" 필드는 모든 패킷이 IPv6이므로 생략가능하고, IPv6 송수신지 주소는 둘 다 링크로컬이므로 인터페이스 ID를 통해 알 수 있고, 하위 64비트 인터페이스 ID 정보는 MAC 계층의 송수신지 주소에서 추정이 가능하므로 역시 생략이 가능하다. 패킷 길이도 IEEE 802.15.4 PPDU 프레임에서 Frame Length를 통해서 또는, 만약 단편화 헤더(fragment header)가 있다면 헤더 내 datagram_size 값을 통해 추정이 가능하다. 트래픽 클래스와 플로우 레이블은 0으로 설정할 경우 생략할 수 있으며, Next Header는 TCP, UDP, ICMP만을 가진다.

IPv6의 헤더 필드 중에서 항상 압축이 되지 않은 상태로 전송되는 유일한 필드는 8비트인 Hop Limit이다. 다른 필드들이 압축되지 않은 상태로 전송되어야 하는지 여부는 IPv6 패킷 헤더가 위의 공통 헤더 부분과 얼마나 다른가에 달려있다. HC1(Header Compression 1)의 비트 5번과 6번은 UDP, TCP 및 ICMP 등에 대한 IPv6 Next Header 필드 영역을 압축할 수 있게 해준다.

2.3 6LoWPAN 단편화 패킷 구조

6LoWPAN 적응계층에서 사용되는 단편화 패킷은 두가지가 정의되어 있다. 첫째는 전체 메시지를 단편화 했을 때 첫 번째로(first) 보내어지는 단편화 패킷 구조와 두 번째 및 계속되어(subsequent) 보내어지는 단편화 패킷 구조이다. 전자의 첫 번째 단편화 패킷의 구조를 그림 3에 나타내었다. 그리고 후자의 두 번째 및 계속된 단편화 패킷의 구조를 그림 4에 나타내었다.

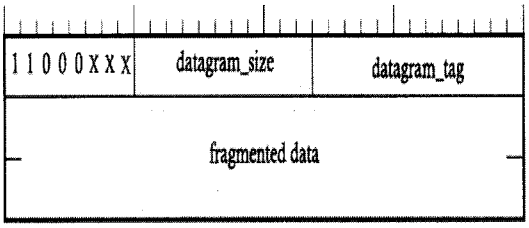

그림 3. 첫 번째 단편화 패킷 구조
Fig. 3. First Fragmented Packet Structure

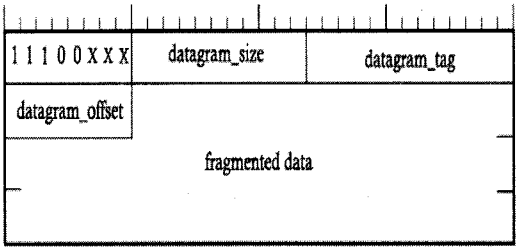

그림 4. 계속된 단편화 패킷 구조
Fig. 4. Subsequent Fragmented Packet Structure

datagram_size는 11비트로 하나의 IPv6 데이터그램이 6LoWPAN 적응계층에서 단편화되어 링크계층에 전달되어져야 할 전체 패킷 사이즈이다. 따라서 하나의 IPv6 데이터그램에 대해 다수로 단편화된 패킷들은 동일한 datagram_size를 갖는다. 이와 유사하게 datagram_tag도 하나의 IPv6 데이터그램이 단편화 되었을 때, 모든 단편화 패킷에 대해 동일한 값이 부여되며, 이 값을 통해 특정 IPv6 데이터그램의 단편화 패킷들임을 구분한다. 초기 값은 정의되지 않았으며, 범위는 0에서 65535까지 이며 1씩 증가되어 부여된다. datagram_offset은 첫 번째 단편화 패킷에는 부여되지 않으며 두 번째와 연속된 단편화 패킷에 대해서만 부여된다. 8바이트 단위로 증가하며 단편의 상대적인 위치를 나타낸다. 따라서 수신측 노드가 임의 순서의 단편화 패킷들을 수신하면, datagram_offset 필드의 값을 기준으로 재조립되어야 하는 지점을 알 수 있다.

III. 단편화로 인한 보안 위협성 분석

이 장에서는 패킷 단편화 및 재조합으로 인해 노출되는 보안 취약점만을 대상으로 공격하는 기존의 공격 기법들을 분석한다. 그리고 이를 기반으로 6LoWPAN 적응계층에서 패킷 단편화 및 재조합으로 인한 보안 취약점을 분석하여 공격 가능성을 분석한다.

3.1 기존의 패킷 단편화를 이용한 공격

기존 IP 또는 TCP 계층에서 패킷 단편화 및 재조합으로 인해 노출되는 보안 취약점만을 대상으로 공격하는 기존의 공격기법은 크게 초소형 단편화(tiny fragmentation) 공격, 단편화 중복(fragment overlap) 공격, 서비스거부 공격, TCP 순서번호 공격 등을 들 수 있다[10~13].

3.1.1 초소형 단편화 공격

보통 20바이트인 TCP 헤더를 2개로 단편화시켜 목적지 TCP 포트번호가 첫 번째 단편화 패킷에 위치하지 않고 두 번째 단편화 패킷에 위치하도록 한다. 패킷 필터링 장비나 침입탐지시스템은 필터링을 결정하기 위해 포트번호를 확인한다. 이 경우에 포트번호가 포함되지 않은 정도로 아주 작게 단편화된 첫 번째 단편화 패킷은 통과되고, 실제 포트번호가 포함되어 있는 두 번째 단편화 패킷은 검사가 되지 않고 통과된다. 결과적으로 보호되어져야 할 목적지 노드에서는 이 패킷들이 재조합되어져 공격자가 원하는 포트의 프로그램으로 무사히 연결될 수 있다. 이런 방법으로 패킷 필터링에서 차단되어져야 하는 패킷을 통과시킬 수도 있고, 침입탐지시스템에서 비정상적인 접속으로 경보되어져야 하지만 전혀 탐지되지 않게 할 수도 있다. 패킷 필터링 장비에 따라 TCP 헤더의 포트번호가 포함되지 않을 정도로 작은 첫 번째 단편화 패킷은 드롭시키기도 한다.

3.1.2 단편화 중복 공격

공격자는 IP 패킷을 두 개의 패킷으로 단편화시킨다. 첫 번째 단편화 패킷에서는 패킷 필터링 장비에서 허용하는 http(TCP 80) 포트를 지정한다. 두 번째 단편화 패킷에서는 offset을 아주 작게 조작해서 단편화 패킷들이 재조합될 때, 두 번째 단편화 패킷이 첫 번째 단편화 패킷 일부분을 덮어쓰도록 한다. 대부분의 공격들은 첫 번째 단편화 패킷의 포트번호가 있는 부분까지 덮어씌운다. 침입차단시스템에서는 첫 번째 단편화 패킷은 허용된 포트번호이므로 통과시키고, 두 번째 단편화 패킷은 이전에 이미 허용된 fragmentation ID를 가진 단편화 패킷이므로 역시 통과시킨다. 이 두 개의 단편화 패킷들이 목적지 노드에 도달되어 재조합된다. TCP/IP 스택은 첫 번째 단편화 패킷의 포트번호가 두 번째 단편화 패킷의 포트번호로 덮어씌어져 있으므로 이 패킷을 필터링되어져야 할 포트의 응용 프로그램으로 전달한다.

3.1.3 서비스 거부 공격

IP 패킷의 단편화는 패킷 필터링이나 침입차단시스템을 우회하는데 이용될 뿐만 아니라 서비스거부공격에도 이용될 수 있다. 이미 잘 알려진 Ping of Death 공격, TearDrop

등이 단편화의 취약점을 이용한 서비스 공격이라 할 수 있다. 이러한 공격은 비정상적인 단편화 패킷들을 재조합하는 과정에서 노드가 정지되거나 재부팅될 수 있다.

Ping of Death나 Jolt 공격은 표준에 규정된 길이 이상으로 큰 IP 패킷을 전송함으로써 수신측 노드가 정상적으로 패킷을 처리하지 못하도록 하거나 상대방 노드를 다운시키는 공격이다. Ping을 이용하여 ICMP 패킷을 정상적인 크기보다 아주 크게 만든 다음 네트워크를 통해 라우팅 되도록 하면, 이 패킷은 공격 네트워크에 도달하는 동안 아주 작은 단편화 패킷 조각이 된다. 공격 대상 노드는 수신된 아주 작은 단편화 패킷을 모두 처리해야 하므로 과부하가 걸리게 된다.

TearDrop, bonk, New TearDrop 공격도 역시 단편화된 패킷의 재조합 과정의 취약점을 이용한 서비스거부 공격이다. 두 번째 단편화 패킷의 offset을 조작하여 단편화 패킷들을 재조합하는 과정에서 버퍼 오버플로우를 유도한다. TearDrop 프로그램은 겹쳐 써진 offset 필드를 가진 단편화 패킷들을 만들어 공격 목표 시스템에 보내며, 공격 목표 시스템은 이러한 단편화 패킷들을 재조합하는 과정에서 정지되거나 재부팅된다.

3.1.4 TCP 순서번호 공격

공격자가 TCP 헤더의 순서번호(sequence number)를 예상해서 TCP 패킷을 임으로 조작하여 자신을 위장하는 방법으로 IP 스푸핑이라는 해킹기법에서 사용된다.

3.2. 6LoWPAN 적응계층에서 패킷 단편화로 인한 보안 위협성 분석

6LoWPAN 적응계층에서는 기존의 IP 패킷 단편화 및 재조합으로 인해 노출되는 보안 취약점을 동일하게 가지고 있다. 추가적으로 다음과 같은 보안 취약점에 새롭게 노출될 수 있다. 만약 공격 의도가 있는 엔티티가 6LoWPAN 단편화 패킷을 송수하는 노드 쌍을 안다면 정상적인 통신을 방해할 수 있다. 예를 들어 공격자가 고의적으로 datagram_offset을 0보다 크게 지정하고 대량의 단편화 패킷을 지정된 특정 주소의 노드로 보낼 경우, 해당 노드는 정상적인 통신을 수행할 수 없다. 이러한 서비스거부 공격은 단편화 패킷들의 소스와 목적지 주소, 프로토콜 번호, 단편화 범위만을 안다면 쉽게 가능해진다.

좀 더 적극적인 공격으로서, 만약 공격자가 특정 경로상에 6LoWPAN 단편화 패킷들을 해석할 수 있다면 다양한 공격들이 가능해진다. 예를 들면 공격자가 원래의 단편화 패킷을 가로채어 단편화 패킷의 datagram_size, datagram_offset, datagram_tag를 직접 조작하거나 재생산하여 통신 경로상에 있는 수신측 노드로 전송하는 공격을 할 수 있다.

현재의 6LoWPAN 표준에서는 단편화를 통해 전송하는 과정에서 단편화된 다수의 패킷들 중, 하나라도 손실이 발생되면 처음부터 재전송이 발생하게 되므로 위와 같은 공격들이 받게 되면 센서 노드는 통신 속도가 매우 느려질 수 있다. 이외에도 수신측 노드가 비정상적인 단편화 패킷들을 재조합하는 과정에서 재조합 버퍼 오버플로우(reassemble buffer overflow), 재전송으로 인한 통신 속도 저하 및 컴퓨팅 자원 손실, 노드 재부팅, 노드 셧다운 등이 유발될 수 있다. 이러한 유형의 공격은 공격자가 숨어서 쉽게 특정 노드를 공격할 수 있다. 또한 앞 절에서 기술한 '기존의 패킷 단편화를 이용한 공격'들도 약간의 변형만을 가하면 6LoWPAN 적응계층에 용이하게 적용할 수 있다.

센서 네트워크 환경은 기존 유선환경이나 상대적으로 전송속도가 높고 대역폭이 넓은 기존의 무선 환경에서보다 이러한 공격들에 대해 훨씬 취약하다고 할 수 있다. 또한, 불필요한 패킷 단편화 및 재조합으로 인해 컴퓨팅 자원이 매우 빠르게 소진될 수 있다. 이러한 취약점들을 대비하지 않을 경우, 센서 노드에 보안 기능이 탑재되었다 하더라도 중요한 응용서비스를 제공하기가 어려워진다.

IV. 제안한 6LoWPAN 재생공격 방지 기법

4.1 기본 가정

6LoWPAN 적응계층에 보안 기능을 탑재하게 되면 보안강도는 높아지지만 단말의 성능저하와 비용이 증가된다. 보안이 요구되는 센서 네트워크 환경을 고려하면 6LoWPAN 적응계층의 특성상 초경량이고 추가적인 컴퓨팅 자원, 메모리, 센서 노드의 가격을 최소화할 수 있는 보안 메커니즘이 필요하다. 이를 위해 추가적으로 탑재되는 패킷의 양과 신호 메시지의 수를 최소화시켜야 한다. 본 논문에서는 기본적으로 6LoWPAN 적응계층에서 최소화된 흐름제어(flow control)가 이루어진다고 가정한다. 즉, TCP 등의 전송계층의 흐름제어를 최소화시켜 6LoWPAN 적응계층에 적용하는 것이다. 이러한 제안의 배경으로서 크게 두가지가 고려되었다. 첫째, 6LoWPAN은 저전력, 낮은 데이터 전송율 그리고 최소형 메모리와 최소형 프로세서만을 장착한 센서 환경이기 때문에 전송계층에서의 재전송을 최소화시켜 전송 효율을 높여야 할 필요가 있다. 둘째, 유선구간과 달리 무선 구간의 특성상 전파에 대한 간섭과 노이즈로 인한 성능저하와, 전송오류, 전파 간섭 등의 영향으로 비트 에러가 높기 때문에, 패킷 손실로 인한 전송계층

(TCP)의 재전송은 정상적인 통신을 방해하는 주요 요인이 될 수 있다. 따라서 하위 계층인 6LoWPAN 적응계층에서 최소한의 흐름제어를 하는 것이 전송계층에서 흐름제어를 하는 것보다 저전력통신과 전송 효율을 높일 수 있다.

제안하는 메커니즘은 재전송을 최소화시켜 저전력 통신을 이루고, 패킷의 신선도 유지 및 재생공격을 방지하는 것을 목표로 한다. 패킷손실이 발생했을 때, 6LoWPAN 적응계층에서 재전송이 이루어지며, 통신선로상에서의 데이터 손실을 검증할 수 있는 체크섬을 도입하여 데이터 무결성을 체크한다. 그리고 재생 공격으로 인한 재전송을 막기 위해 타임스템프와 난스를 도입하였다.

4.2 동작흐름

하나의 IPv6 데이터그램이 다수의 단편화된 패킷들로 조각되어 전송되는 경우에, 그리고 중간의 단편화 패킷의 일부가 손실되었다고 가정했을 때, 제안하는 메커니즘의 재전송 절차를 그림 5에 도시하였다. 구체적인 하나의 예로서, 6LoWPAN 계층에서 전송해야 할 하나의 데이터그램 사이즈가 800바이트이고, 6LoWPAN 적응계층에서는 80바이트로 단편화 되어 전송되어진다고 가정한다. 우선 송신측 노드에서 단편화된 패킷 각각에 대해 순서번호 FSN(Fragmented Sequence Number)를 부여한다. 이 경우에는 단편화된 패킷 단위로 FSN이 10번까지 부여된다. 그림 5의 절차는 FSN 10번까지의 단편화된 패킷이 송신측 노드에서 수신측 노드로 전송되는 도중에 FSN 9번의 단편화 패킷이 손실되어 재전송되는 흐름을 보여주고 있다. 전체 흐름을 4단계로 분류하여 기술한다.

첫 번째 단계는 단편화 패킷 전송단계로서, 송신측 노드는 데이터그램을 단편화시키고 datagram_offset을 기준으로 FSN을 계산한다. 그리고 FSN 1번에서 마지막 전의 단편화 패킷까지 즉, FSN 9까지의 단편화 패킷 내에 타임스템프를 포함시켜 전송한다. 그리고 마지막 단편화 패킷은 무결성을 체크하기 위해 체크섬을 포함시켜 전송한다. 여기까지의 절차는 6LoWPAN 표준문서[1]에서 정의한 절차와 동일하다. 단, 타임스템프, 난스, 체크섬 필드를 추가시켜 전송하는 점이 다르다.

수신측 노드는 단편화 패킷들을 수신하면 기본적으로 하나의 데이터그램에 대해 하나의 FSN 테이블을 생성한다. 이 테이블은 최대 32비트를 가지며 각 비트는 순서대로 FSN 단위로 단편화 패킷의 수신상태를 저장하고 관리한다. 테이블의 특정 비트가 1로 지정되어 있으면 해당 FSN 단편화 패킷은 정상적으로 수신된 것으로 의미를 부여한다. 따라서 0으로 지정되어 있으면 해당 FSN 단편화 패킷이 정상적으로 수신되지 않은 것이다.

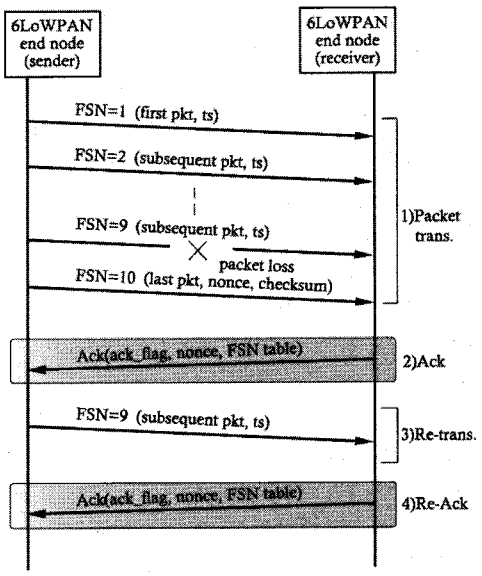

그림 5. 제안하는 재전송 절차
Fig. 5. Proposed Re-transmission Procedure

마지막 단편화 패킷을 모두 수신했을 때, FSN 테이블을 읽어보면 전체 단편화 패킷들이 정상적으로 수신되었는지 또는, 특정 FSN 단편화 패킷이 손실되어 수신되지 않았는지를 판단할 수 있다. 그리고 수신측 노드는 datagram_size를 기준으로 전체 수신해야 할 FSN을 계산하고 이를 기준으로 동적 메모리를 할당한다. 최초 패킷부터 버퍼링을 시작하고, 마지막 패킷을 수신하였을 때는 체크섬을 통해 무결성을 확인하고 통신 선로상에서 손실된 FSN 번호를 계산한다.

마지막 단편화 패킷을 정상적으로 수신하였을 경우는 계산된 FSN 테이블에 모든 비트를 1로 지정한다. 이때 만약 마지막 단편화 패킷이 손실되어 수신하지 못했을 경우가 발생할 수 있다. 이 경우 연속되는 FSN 단편화 패킷들의 타임스템프를 비교하여 RTT(Round Trip Time)를 계산하여 마지막 단편화 패킷의 손실을 판단한다. 만약 손실되었을 경우, FSN 테이블의 마지막 FSN을 0으로 지정한다.

두 번째 수신측 노드는 단편화 패킷들의 수신상태를 나타내는 FSN 테이블을 응답(Ack)메시지에 포함시켜 성공적인 데이터그램의 수신을 알리거나 또는, 특정 단편화 패킷이 손실되었음을 송신측에 알려 재전송을 요청하는 응답 단계이다. 세 번째는 재전송 단계로서, Ack 메시지를 받은 송신측 노드는 FSN 테이블을 체크하여 재전송이 필요한 FSN 단편화 패킷들을 파악한다. FSN 테이블의 모든 비트가 1로 지정되어 있으면 전체 단편화 패킷들을 수신측 노드가 정상적으로 수신

하였으므로 재전송이 필요 없으며 절차를 종료한다. 만약 FSN 테이블의 특정 비트가 0으로 지정되어 있으면 해당 단편화 패킷들만을 수신측 노드로 재전송한다.

마지막 네 번째 단계는 재전송의 응답 단계로서, 수신측 노드가 재전송을 받은 단편화 패킷들을 체크하여 정상적으로 수신했는지를 FSN 테이블에 지정하여 재응답을 하는 것이다. 만약 재전송에서도 패킷손실이 발생하면 추가적인 재전송을 요청한다. 통신 중에 하위 계층의 통신 단락을 고려하여 재전송 최대 횟수는 제한적이어야 한다. 재전송 최대 횟수는 상위 전송계층(TCP)의 재전송 타임아웃(re-transmission time out)를 고려하여 지정되어야 한다.

4.3 Dispatch 헤더 정의

표 2. 제안한 디스팻치 헤더 패턴
Table 2. Proposed Dispatch Header Pattern

패턴	패턴 이름	의미
00xxxxxx	NLAP	Not a LoWPAN Frame
01000001	IPv6	Uncompressed IPv6 Address
01000010	LOWPAN_HC1	LOWPAN_HC1 Compressed IPv6
01010000	LOWPAN_BC0	LOWPAN_BC0 Broadcast
10xxxxxx	MESH	Mesh Header
11000xxx	FRAG1	Fragmentation Header(first)
11000001	FRAG1_Re	Fragmentation Header(first, timestamp)
11100xxx	FRAGN	Fragmentation Header(subsequent)
11100001	FRAG_Re	Fragmentation Header(subsequent, timestamp)
11100010	FRAGL	Fragmentation Header(last, timestamp, checksum)
11100011	FRAGACK	Fragmentation Header(ack_flag, nonce, FSN table)

6LoWPAN 표준[1]과의 호환성을 고려하여, 제안하는 메커니즘을 지원하기 위해서 필요한 추가적인 헤더 패턴을 표 2에 정의하였다. 4개의 단편화 헤더 패턴이 추가되었다. FRAG1_Re는 첫 번째 단편화 패킷을 나타내는 헤더 패턴이며, FRAGN_Re는 두번째 이후 계속되는 단편화 패킷을 나타내는 헤더 패턴이며, FRAGL_Re는 마지막 단편화 패킷을 나타내는 헤더 패턴이며, FRAG_ACK는 단편화 응답을 나타내는 헤더 패턴이다.

4.4 단편화 패킷 구조 및 필드 추가

첫 번째 단편화 패킷 헤더를 그림 6에 나타내었다. Dispatch 11000001에 의해 첫 번째 단편화 패킷이 구분되며, 6LoWPAN 표준문서에 정의된 첫 번째 단편화 패킷헤더에 비해 타임스템프가 추가된다.

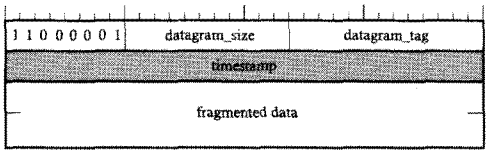

그림 6. 첫 번째 단편화 패킷 구조(FRAG1_Re)
Fig. 6. First Fragmented Packet Structure(FRAG1_Re)

두 번째 이후 계속된 단편화 패킷 헤더를 그림 7에 나타내었다. Dispatch 11100001에 의해 계속된 단편화 패킷이 구분되며, 6LoWPAN 표준문서에 정의된 첫 번째 단편화 패킷 헤더에 비해 FSN과 타임스템프가 추가된다.

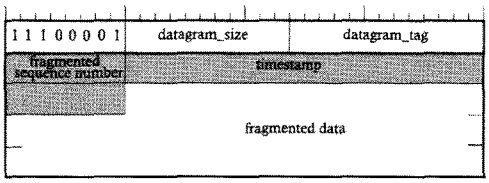

그림 7. 계속된 단편화 패킷 구조(FRAGN_Re)
Fig. 7. Subsequent Fragmented Packet Structure(FRAGN_Re)

마지막 단편화 패킷 헤더를 그림 8에 나타내었다. Dispatch 11100010에 의해 마지막 단편화 패킷이 구분되며, 6LoWPAN 표준문서에는 이와 같은 마지막 단편화 패킷 헤더가 별도로 정의되지 않았으나 본 논문에서는 무결성 체크를 위해 추가되었다. 그림 8에 정의된 마지막 단편화 패킷헤더는 6LoWPAN 표준문서에 정의된 계속된 단편화 패킷헤더와 비교하여 난스와 체크섬이 추가된다.

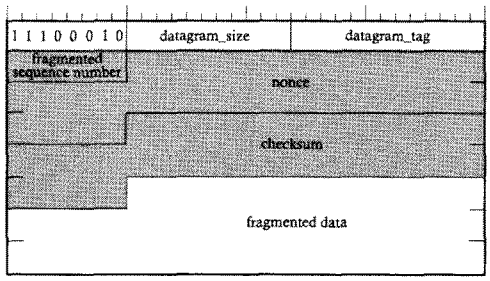

그림 8. 마지막 단편화 패킷 구조(FRAGL)
Fig. 8. Last Fragmented Packet Structure(FRAGL)

단편화 응답 패킷 헤더를 그림 9에 나타내었다. Dispatch 11100011에 의해 단편화 응답 패킷이 구분되며, 6LoWPAN 표준문서에는 정의되지 않았으며 본 메커니즘을 위해 별도로 추가 정의하였다.

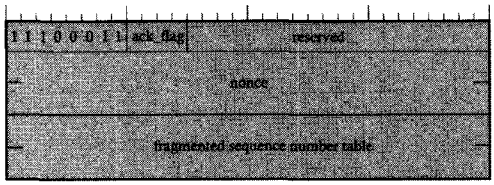

그림 9. 응답 단편화 패킷 구조(FRAGL)
Fig. 9. Ack Fragmented Packet Structure(FRAGL)

4.4.1 타임스템프(timestamp)

재생공격에 의한 재전송을 막기 위하여 단방향의 단편화된 패킷(unidirectional fragmented packet)에 타임스템프를 포함시킨다. 즉, 첫 번째 단편화 패킷, 두 번째 이후 계속된 단편화 패킷, 그리고 재전송시에도 이들 두가지 단편화 패킷에 동일하게 타임스템프를 포함시킨다. 타임스템프 사이즈는 저속으로 데이터가 송수신되는 점과 타임스템프를 포함에 따른 패킷의 사이즈를 최소화시키기 위해 32비트로 구성하였다. 그러나 필요하다면 48비트(초)와 16비트(1/64초)로 이루어진 전체 64비트로 구성할 수도 있다.

4.4.2 FSN(fragmented sequence number)

송신측에서 하나의 데이터그램을 단편화시킬 때, 하나의 단편화 패킷마다 순서번호를 부여한다. 필드의 사이즈는 8바이트이며 초기 값은 0이며 최대 순서번호는 256까지 지정된다. 수신측 노드에서 재조합을 하기 위해서는 단편의 상대적 위치(datagram_offset)가 필요하며 다음과 같이 계산한다.

$$datagram\_offset = FSN \times \max\_fragmented\_size$$

4.4.3 난스(nonce)

재생공격에 의한 재전송을 막기 위하여 양방향의 단편화된 패킷(bidirectional fragmented packet)에는 난스를 적용한다. 타임스템프는 매 단편화 패킷마다 포함되므로 데이터 사이즈가 최소화 되어야 하나, 난스는 한 개의 데이터그램에 두 개의 난스 필드가 포함되므로 사이즈에는 큰 영향을 받지 않는다. 이를 고려하여 64비트를 적용하였다. 그러나 패킷 사이즈를 더욱 최소화하기 위해서는 32비트도 지정할 수 있다.

4.4.4 체크섬(checksum)

마지막 단편화 패킷에는 전체 데이터그램에 대한 무결성을 검증하기 위해 체크섬을 포함시킨다. 모든 단편화 패킷에 체크섬을 포함시키면 오버헤드가 너무 커지므로 마지막 단편화 패킷에만 포함시킨다. 이 필드는 단편화되지 않은 데이터그램 전체와 6LoWPAN 헤더를 포함시켜 계산한다. 체크섬 필드는 단편화된 마지막 패킷에만 삽입되며 다음과 같이 계산한다. 체크섬 필드의 초기 값은 0으로 설정한다. 그런 다음 헤더의 16비트에 대한 1의 보수합이 계산된다. 이 합에 16비트 1의 보수값은 체크섬 필드에 저장된다. 최종적으로 헤더의 16비트 1의 보수합을 계산한다.

4.4.5 FSN 테이블(fragmented sequence number table)

단편화하지 않은 데이터그램은 FSN 테이블을 생성하지 않으며, 단편화가 이루어질 때만 하나의 데이터그램에 대한 테이블을 생성한다. 단편화 패킷을 수신한 노드측에서 생성하는 테이블로서, 32비트를 가지며 각 비트는 순서대로 FSN 단위로 단편화 패킷의 수신상태를 저장하고 관리한다. 테이블의 특정 비트가 1로 지정되어 있으면 해당 FSN 단편화 패킷은 정상적으로 수신된 것이며, 0으로 지정되어 있으면 해당 FSN 단편화 패킷이 정상적으로 수신되지 않은 것이다.

4.4.6 응답 테이블(ack_flag)

응답 플래그는 수신측 노드가 송신측 노드에게 응답을 요구하는지 상태를 나타내는 상태 플래그이다. 4개의 상태가 존재하며 이 외에도 필요에 따라 추가시킬 수 있다.

- 0000 : not used
- 0001 : no reply required
- 0011 : re-transmission required
- other : reserved

V. 성능 분석

제안한 메커니즘의 재전송 지연 시간을 분석하였다. 6LoWPAN 적응계층에서 단편화가 발생했을 때, 하위 계층인 IEEE 802.15.4 MAC/PHY에서의 에러 확률에 따른 6LoWPAN MTU의 전송시간과 홉 수에 따른 전송시간을 계산하였다. 다중 홉 일 경우에는 다양한 네트워크 토폴로지가 아닌 단일경로를 가정하였으며, 재전송 타임아웃, 재조립 버퍼에 의한 지연은 고려하지 않았다. 여기서 6LoWPAN MTU는 6LoWPAN 헤더, 제안 메커니즘의 단편화 헤더, 상위의 IP, TCP, 그리고 응용계층이 포함된 데이터를 의미한다. 하나의 MTU가 송신측 노

드에서 수신측 노드로 전달되는 전체 전송시간은 다음과 같이 계산할 수 있다[6].

$Trns$

$$\times \frac{(T_{frg} \times M_{nfrag}) + (N_{hop} \times D_{pro})}{(1-p_e)^{N_{hop}}}$$

여기서 p_e는 전송 에러 확률, $Trns$ 는 하나의 MTU 전체 전송시간, M_{nfrag}는 하나의 MTU에 대한 단편화 개수, T_{frag}는 단편화 패킷 전송시간, D_{pro}는 홉과 홉 사이의 전파지연, N_{hops}는 홉 수, N_{retrns}는 재전송 횟수의 평균값이며 아래와 같이 계산된다.

$$N_{retrns} = \frac{1}{(1-p_e)} \quad 0 \le p_e < 1$$

그림 10에 IEEE 802.15.4 MAC/PHY의 전송 에러 확률 p_e가 0에서 1까지 변화되었을 때, 홉 수를 1개에서 5개까지 고려하여 전체 MTU 재전송 지연 시간을 나타내었다. 분석에서 T_{frag}=10msec, D_{pro}=5msec, M_{nfrag}=10을 초기 값으로 지정하였다. 초기 값과 관련하여 IEEE 802.15.4의 유효전송 속도 100kbps를 고려하여 T_{frag}를 10ms로, 그리고 홉간 전파 지연시간 D_{pro}는 참고문헌 [14]를 참조하여 5ms를 지정하였다. 그리고 MTU 최대 크기가 2Kbyte이고 보안 기능이 탑재될 경우, 유효 페이로드는 80바이트가 된다. 따라서 단편화 패킷의 수는 25개 된다[2]. 분석에서는 중간 크기의 MTU를 고려하여 M_{nfrag}는 10을 지정하였다.

분석 결과에 의하면 전송에러가 높아질수록 즉, 패킷 손실이 높아질수록 재전송이 급격하게 증가한다. 또한 홉 수가 증가함에 따라 재전송이 비례적으로 증가함을 알 수 있다. 참고로 센서 네트워크를 위한 라우팅 프로토콜들은 일반적으로 최대 10개 이내의 홉 수를 고려하고 있다. 분석 결과에서는 홉 수를 5개로 한정하여 결과를 제시하고 있으며 홉 수가 그 이상이 되어도 비례적으로 증가한다.

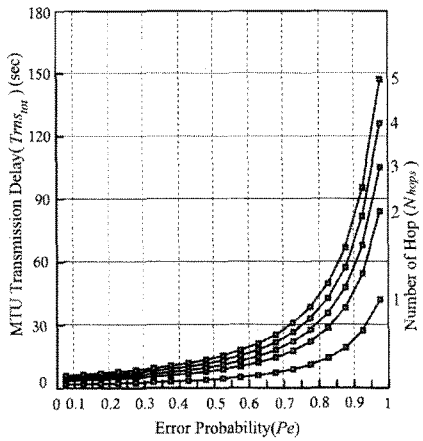

그림 10. 홉 수에 따른 MTU 재전송 지연
Fig. 10. Re-transmission Delay by the Number of Hop

그림 11에 IEEE 802.15.4 MAC/PHY의 전송 에러 확률 p_e가 0에서 1까지 변화되었을 때, 단편화된 패킷의 개수에 따른 전체 MTU 재전송 지연 시간을 나타내었다. 분석에서 초기 값은 위와 동일하게 T_{frag}=10msec, D_{pro}=5msec, M_{nfrag}=10으로 지정하였으며, 단편화 패킷 수를 10개, 50개, 100개, 200개, 400개로 변경하여 적용하였다. 80바이트인 단편화 패킷이 10개이면 하나의 MTU는 800바이트에 해당된다. 그림 10과 유사하게 단편화 패킷의 개수가 증가할수록 재전송이 급속히 증가한다. 결과에 의하면 그림 10과 유사하게 단편화 패킷의 개수가 증가할수록 재전송이 급속하게 증가함을 알 수 있다.

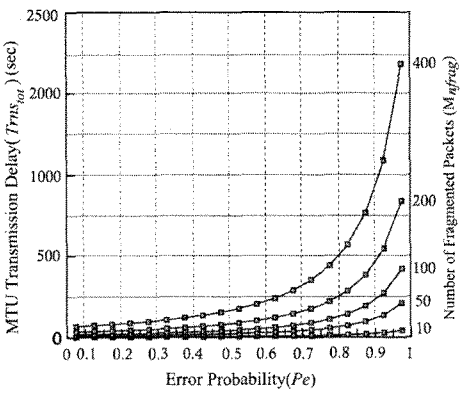

그림 11. 단편화 패킷 수에 따른 전송 지연
Fig. 11. Re-transmission Delay by the Number of Fragmented Packets

VI. 결론

본 논문에서는 6LoWPAN 계층에서 패킷 단편화 및 재조립으로 인해 발생할 수 있는 보안 취약점을 분석하고 이를 기반으로 재생공격으로 인한 재전송을 최소화할 수 있는 메커니즘을 제안하였다. 6LoWPAN 표준을 기반으로 추가적인 재전송 절차 및 단편화 패킷 구조를 설계하였다. 그리고 제안한 메커니즘의 성능을 평가하기 위해 재전송 지연시간을 분석하였다. 분석결과에 의하면 전송에러가 높아질수록 즉, 패킷 손실이 높아질수록 재전송이 급격하게 증가하고 또한, 홉 수가 증가함에 따라 재전송이 비례적으로 증가함을 알 수 있었다. 메커니즘의 장점은 불필요한 패킷 단편화와 재조립을 최소화하여 센서 노드의 통신 환경에 대한 신뢰성을 높일 수 있다. 추후 TCP 응용서비스를 탑재하고 실제 6LoWPAN에서의 재전송이 TCP 재전송에 미치는 영향을 분석하는 연구가 필요하다.

참고문헌

[1] G G. Montenegro, N. Kushalnager, etc., "Transmisson of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC4944, September 2007.

[2] IETF, "IPv6 over Low power WPAN(6LowPAN), *"http://www.ietf.org.*

[3] IEEE Computer Society, "IEEE std. 802.15.4-2003", October 2003.

[4] IEEE, "802.15.4 Wireless Medium Access Control (MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks(LRWPANs), " IEEE Computer Society, September 2003.

[5] S. Diniel Park, K. Kim, E. Seo, S. Charkrabarti, "IPv6 over Low Power WPAN Security Analysis," IETF draft-daniel-6lowpan-security- analysis-02.txt", June 2006.

[6] G. P. Chandranmenon and G. Varghese, "Reconsidering fragmentation and reassembly," 17th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, 1998.

[7] Adam Dunkles, Juan Alonso, Thiemo Voigt, and Hartmut Ritter, "Distributed TCP Caching for Wireless Sensor Networks," MedHocNet2004, December 2004.

[8] Y. Sankarasubramaniam, etc., "ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks," MobiHoc 2003, 2003.

[9] Chieh-Yih Wan, Shane B. Eisenman, Andrew T. Campbell, "CODA: Congestion Detection and Avoidance in Sensor Networks," SenSys 2003, November 2003.

[10] CERT CC-KR Technical Report, "IP Fragment를 이용한 공격기술," *http://cert.cc.or*, 2001.

[11] C. A Kent and J. C. Mogul, "*Fragmentation considered harmful,*" WPL Technical Report 87/3, December 1987..

[12] Jason Anderson, "An Analysis of Fragmentation Attacks," *www.sans.org*, March 2001.

[13] H. G. Kim, "Protection against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer," ICHIT 2008, pp.796-801, August 2008.

[14] 최낙중 외 5명, "IEEE 802.11 기반 무선랜에서 TCP 인지 서버 계층 TAS," 정보과학회 논문지 제 33권, 제 5호, 355-368쪽, 2006년 10월.

저자소개

김 현 곤

1992년 : 금오공과대학교 전자공학과 학사

1994년 : 금오공과대학교 전자공학과 공학석사

2003년 : 충남대학교 전자공학과 공학박사

1994~2005년 : 한국전자통신연구원 정보보호연구단 팀장

2005년~현재 : 목포대학교 정보보호학과 조교수

관심분야 : RFID/USN 보안, 이동통신 보안, 차량통신 보안