USN 미들웨어의 정보 보호 기술을 위한 워터마킹 처리 연구

노창배*, 송주빈**, 변시우***
경희대학교 전파공학과*, 경희대학교 전파공학과**, 안양대학교 디지털미디어공학과***

The watermarking control research for information protective techniques of USN middleware

Chang-Bae Roh*, Ju-Bin Song**, Si-Woo Byun***
Dept of Radio Engineering, KyungHee University*, Dept of Radio Engineering, KyungHee University**,
Dept of Digital Media, Anyang University***

Abstract - 본 논문은 USN 미들웨어에서 정보보호를 위한 워터마킹에 대한 처리 기술 개발을 목표로 한다. 기존의 USN과 정보보호기술에 대해 분석하고, 이를 워터마킹을 이용한 관점에서 정보보호 처리기술을 연구 분석한다. 디지털 영상에 워터마크를 삽입해 영상이 원본인지 아닌지 확인하는 기술을 응용해 USN의 미들웨어에서 효과적으로 활용하고, 이를 응용한 정보보호기술에 대해 제안한다.

1. 서 론

IT 강국, 세계 최고의 인터넷 통신 인프라망을 구축해서 앞으로 비전이 있지만, 이러한 이름 뒤에는 바이러스와 악성코드, 개인 정보 유출이 난무하는 통신망을 갖추고 있다는 오명을 갖고 있다.

정보통신기술의 발전과 인터넷 이용 확산 등으로 얼마나 개인 정보를 유출하지 않고, 잘 보호할 수 있느냐가 화두가 되었다.

기존에는 패스워드 또는 PIN(Personal Identification Number)을 이용한 사용자 인증 방법이 편리하게 사용되었으나, 이러한 방법은 개인 정보를 유출할 수 있다는 점에서 여러 가지 문제점을 가지고 있다[1].

개인 정보 유출에 대한 문제를 해결하게 위해 다양한 형태의 인증 방법에 연구/개발되고 있지만, 100% 정확히 막을 수 있는 방법은 없다. 현재 개발/구현되고 있는 분야는 디지털 컨텐츠를 보호할 때 사용되는 워터마킹 처리 기술로, 이를 이용해 정보의 유출을 확실히 보호하고자 한다.

본 연구에서는 USN 미들웨어에서의 정보보호라는 관점에서 워터마킹기술을 어떻게 적용할지에 대해 제안하고자 한다.

2. 본 론

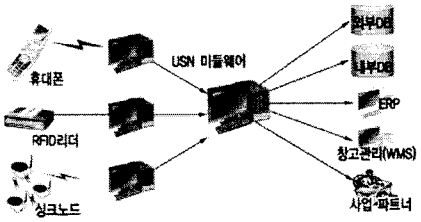
먼저, 워터마킹 처리 기술을 요즘 화두로 떠오르고 있는 USN(Ubiquitous Sensor Network)과 접목해서 모든 사물에 태그를 부착하고, 사물 정보 및 환경 정보까지 감지하고, 네트워크를 통해 실시간으로 관리하는데 사용자 정보를 누출하지 않고, 정보 보호를 하는데 목적을 가진다.

기존에는 인간 중심의 정보화 사회가 사람과 사물뿐만 아니라, 사물 사이에도 정보들이 유기적으로 결합되고 활용될 수 있는 유비쿼터스 컴퓨팅 사회로 변모하고 있다.

유비쿼터스 컴퓨팅 사회에서 사물들은 센서를 이용해 새로운 형태의 정보를 생성하고, 이렇게 생성된 정보는 미들웨어를 통해 서버에 전달되어 메시지를 처리한다.

2.1 USN 미들웨어의 개념

USN 미들웨어에 대한 개념도는 다음과 같다.

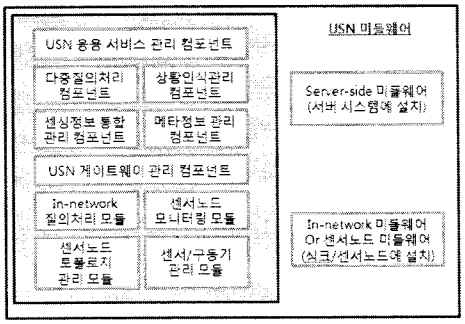


〈그림 1〉 USN 미들웨어 개념도

2.2 USN 미들웨어 시스템

유비쿼터스시대 도래에 대비한 u-지역 정보화 시범사업으로는 "u-상수도 시설관제", "u-Healthcare시스템", "RFID /USN기반의 u-화재예방시스템", "모바일차고지 증명제 시스템" 등 u-지역주민서비스 등이 있다.

〈그림 1〉 USN 미들웨어 시스템의 기본 구성



<출처 : USN 미들웨어 기술개발 동향, ETRI 2007>

이러한 유비쿼터스의 궁극적인 목적은 u-City의 구축으로 이는 행정, 의료, 교통, 물류, 정보가전, 환경, 재난방재 등의 도시 환경을 이루는 필수 요소들에 대한 편의를 증대시키는데 목적을 둔다[2].

<그림 3> u-City내 USN 응용서비스의 범위

USN 응용 서비스	u-City 활용 서비스
설비, 교통	설비 관리, 교통
유통, 물류	자산관리/경영지원, 유통/물류
환경	환경
자동화, 안전	주거관리, 행정
생활, 문화	건강관리, 교육, 행정

<출처 : USN 응용서비스 동향, ETRI 2007>

USN을 이용해 u-City를 구축하는데 있어 고려해야할 시

스템은 다음과 같다.

- 해커가 태그의 정보 획득을 시도하는 공격을 막는 인증 처리 시스템
- Reader와 Tag 사이의 데이터교환 도청방지 시스템
- 데이터 위조를 하는 Reader 또는 Tag를 혼란시키는 공격을 방어하는 데이터 기밀성과 무결성 보장시스템
- Reader에 대한 DoS 공격을 감지 및 방지 시스템
- RFID/USN을 구성하는 서버에 대한 트래픽 폭주 제어 기술 시스템
- RFID/USN 네트워크 노드 사이의 신뢰 채널 시스템
- 센서 신호에 대한 Jamming 회피 시스템

USN 미들웨어는 USN 응용시스템과 센서노드 사이에 위치하는 것으로 둘 사이에 데이터를 효율적으로 전달할 수 있도록 하는 역할을 수행한다. 대부분의 USN 미들웨어는 서버측 미들웨어 또는 센서노드 미들웨어로 구분이 된다.

이중 서버측 미들웨어는 다수의 USN 응용서비스 관리, USN 응용서비스 다중질의 서비스, 센싱 정보와 메타 정보에 대한 효율적 관리 서비스 등을 수행한다.

또한, 센서노드 미들웨어는 센서노드와 싱크노드 수준에서 질의어를 처리하고, 센서노드 사이의 네트워크를 위한 토폴로지 정보를 관리한다. 이외에도 센서노드의 상태 정보를 관리할 수 있다.

2.3 USN과 센서노드의 정보보호

인터넷이 급속히 확산되고 현대 생활에서 필수제로 자리잡은 까닭은 표준화된 식별체계(IP), 전송방식과 데이터 교환절차(프로토콜) 등이 잘 정의됐기 때문이다. 이와 유사하게 USN과 인터넷간, USN 상호간의 정보교환이 원활하기 위해서는 공통의 USN 식별체계, 표준 프로파일, 데이터 통신 절차, 데이터 형식 등이 마련돼야 한다.

기업내 자산에 자산관리번호가 부여되듯 u-센서와 USN 자원을 식별할 수 있는 식별체계, 프로파일을 정의하고 부여하는 것이다. 또한 u-센서를 관리하기 위한 주요 프로파일을 표준화하고, 이를 국제 표준화함으로써 USN 기술을 선도할 수 있다[3].

USN은 센서노드들 사이의 무선 통신으로 구성되기 때문에 Tag에서 전달된 데이터를 센싱하는 정보가 다른 사람에게 도청을 당하거나 엉뚱한 값으로 바뀔 가능성이 높다. 따라서 USN의 미들웨어는 센서노드 미들웨어에서 센서노드들과 게이트웨이 사이에서 센싱 정보를 보호하기 위한 방법을 제공한다[4].

이때, 고려해야 할 점이 있다면 정보보호 기능을 구현하면서 효율성을 위해 센서 노드의 자원에 대한 점유율을 최소화해야 한다. 물론 정보보호 기능을 구현하면서 워터마크 기술과 최신 암호화 기술이 적용되어야 할 것이다.

2.4 미들웨어에 워터마크 삽입과 추출

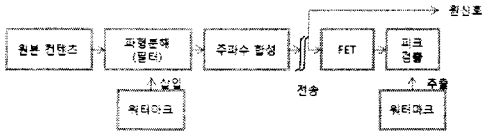
디지털 정보의 저작권을 보호하는 방법에는 전송선로 단계에서 디지털 정보에 대한 암호화를 취하는 방법, 디지털 정보의 불법적인 내용 조작을 방지하고 소유권을 보호할 수 있는 디지털 워터마크(watermark) 방법, 그리고 방화벽(firewall)과 같이 접근을 원천적으로 제어하는 방법이 있다.

워터마크는 저작권 보호를 위해 사람이 인식할 수 없는 멀티미디어 정보의 보이지 않는 변화된 값이며, 워터마크를 멀티미디어 정보에 사람이 인지할 수 없도록 저장하는 행위이다.

특히 디지털 영상을 워터마킹할 경우 반드시 고려해야 할 특징으로써는 워터마크가 첨가된 영상에서 워터마크를 인지할 수 없어야 한다는 무감지성(invisibility), 불법적인 도용이 불가능하여야 한다는 보안성(security), 워터마킹된 영상은 외부의 어떠한 변형(attack)에도 워터마크가 지워져서는 안되는 강인성(robustness), 그리고 명확하게 소유권을 증명할 수 있는 방법을 제시해야 하는 명확성(unambiguity)이 있다.

이러한 워터마킹기술은 인터넷상에서 제공하기 어려운 형태의 성적 증명서나 은행 잔고 증명서 등에서 사용되고, 온라인 티켓이나 상품권 발급 서비스 등에서 널리 보급되어 있다. 또한, 디지털 영상과 음악 제작을 할 때 저작자의 로고나 상표, 인감, 서명 등에 대한 정보를 삽입할 수도 있다. 최근에 디지털 워터마킹 기술은 데이터 은닉이나 암호화 등의 관련 분야로 응용이 확산되고 있는 추세이다.

이러한 기법들을 USN 미들웨어에 사용하면 필터링과 압축 등에 의한 정보의 변형이 되지 않고, 숨겨진 데이터에 의해 원본 데이터가 커지지 않는다. 또한, USN의 불법 사용자나 정보의 불법 유출에 대비한 검출, 삭제, 수정이 불가능하다.



〈그림 4〉 워터마크 삽입/추출 구성도

미들웨어에서 워터마크 기법을 이용할 때 검출 방법은 공개 워터마킹 검출과 비공개 워터마킹 검출로 구분된다. 우선 공개 워터마킹은 검출하고자 하는 알고리즘을 공개하기 때문에 모든 사용자가 워터마크를 검출은 할 수 있지만, 생성/제거는 할 수 없다. 하지만, 비공개 워터마킹은 알고리즘 자체를 공개하지 않고, 워터마크를 검출하기 때문에 원본에 대한 데이터가 필요하다는 특징이 있다.

3. 결 론

기존에 USN 미들웨어에서 정보 보호를 하기 위해 다양한 방법론이 거론되고 있다. 본 연구에서는 이러한 방법들 중에서 디지털 컨텐츠를 보호를 위해 사용되고 있는 'WS-DVR' 디지털 영상에 눈에 보이지 않는 워터마크를 삽입, 필요시 해당 영상이 원본인지 아닌지 확인할 수 있음은 물론 만약 위/변조된 영상으로 판명됐을 경우 그 위치까지 정확히 알려줄 수 있다.

이러한 기술을 디지털 영상에서만 사용하는 것이 아니라, USN의 미들웨어까지 끌고 와서 개인적인 정보를 보호할 수 있다면 앞으로 불투명한 미래 정보 사회에 큰 활력을 가져올 수 있다. 따라서 본 논문에서는 USN 미들웨어의 정보 보호 기술을 위한 워터마킹 처리에 대한 기법을 제안하였다.

[참 고 문 헌]

[1] 김태해, 정승환, 정용화, 문대성, 문기영, "워터마킹 기법을 이용한 생체정보 보호", 정보보호학회, 15권 6호, 2005.

[2] Salem Hadim and Nader Mohamed, "Middleware Challenges and Approaches for Wireless Sensor Networks," IEEE Distributed Systems Online, Vol.7, No.3, 2006.

[3] 안철현, "USN 정보자원 관리 프레임워크 제안", 온더넷, 2006.

[4] 김민수, 이용준, 박종현, "USN 미들웨어 기술개발 동향", 전자통신동향분석 22권, 3호, 2007.