CCTV 대체용 네트워크 카메라의 보안 강화를 위한 다중 접근권한 프락시 서버 구현

Proxy Server Providing Multi-level Privileges for Network Cameras on the Video Surveillance System

배 광 진* 이 경 률** 임 강 빈***
Kwangjin Bae Kyungroul Lee Kangbin Yim

요 약

본 논문은 영상감시용 네트워크 카메라가 원격지에 설치됨으로써 보안 환경 및 갱신으로부터 소외되어 발생하는 보안 취약성을 지적하고 이를 해결하기 위한 방안으로 네트워크 카메라로의 안전한 접속을 대행하기 위한 보안 프락시 서버 구조를 제안한다. 제안한 서버는 보안 네트워크상에 위치하여 대규모 네트워크 카메라 군에 대한 접속정보를 은닉하고 보안 관리자를 통하여 접속을 시도하는 클라이언트를 인증한다. 또한 그룹 키를 기반으로 하는 영상정보의 암호화 및 키의 갱신 기능을 통하여 영상정보에 대한 등급 지정과 클라이언트에 대한 등급별 안전한 영상 서비스를 제공한다. 제안한 서버를 다중의 네트워크 카메라를 대상으로 구현하여 실험함으로써 네트워크 카메라에 직접 접속하는 경우와 동등한 품질의 영상 서비스를 유지하면서 네트워크 카메라를 안전하게 보호할 수 있음을 확인하였다. 본 연구의 결과를 통하여 임의 접근이 가능한 기존의 네트워크 카메라에 대하여 안전하고 일관된 통합관리가 가능해질 것으로 사료된다.

ABSTRACT

This paper introduces security problems on the video surveillance systems where the network cameras are equipped at remote places and isolated from the updated and secure environment and proposes a framework for a proxy server that is delegated to connect to network cameras by providing a secure connections from the clients. The server in the framework is deployed within a secure network, secretes the information for connection to cameras and authenticates the clients. Additionally, it provides a secure video service incorporating multi-level privileges for both images and clients through a encryption key distribution and management facility. Through an implementation of the server and a its deployment , it was proved that In this server implement to multi network camera and we confirm compare direct access to network camera equal video quality of service and it can be protection network camera. We expect that can be secure and integral management about traditional network camera through experimental result.

☞ keyword : CCTV, proxy server, network camera, video surveillance, access control, key sharing

1. 서 론

생활이 복잡해지고 활동 범위가 확대되면서 도로, 건물 등 감시가 필요한 중요 지점에 설치된 네트워크카메라 기반의 감시 시스템을 빈번히 볼 수 있다. 이러한 감시 시스템은 초기 설치비가 저렴하고, 유지비를 요구하지 않으며, 확장성이 뛰어난 제품으로 최고의 보안 장비로 각광받고 있다.

네트워크카메라는 설치 공간과 비용, 안정성 등의 문제로 인하여 임베디드시스템을 기반으로 구성된다. 이러한 무수히 많은 네트워크카메라에 대하여 영상정보에 접근하거나 장치를 관리하기 위해서는 많은 제약이 따른다. 네트워크카메라에 직접 접속을 할 경우 접속자 수에 대한 제한과 임

* 정 회 원 : (주) 기가레인 연구원
kjbae@sch.ac.kr
** 정 회 원 : 순천향대학교 정보보호학과 박사과정
carpedm@sch.ac.kr
*** 종신회원 : 순천향대학교 정보보호학과 교수
yim@sch.ac.kr
[2010/11/14 투고 - 2010/11/22 심사 - 2011/02/28 심사완료]

베디드 환경에 따른 자원의 부족 그리고 복수의 네트워크카메라에 대한 접속이 불가하다는 단점이 있다. 또한 기존의 네트워크카메라는 보안에 있어서도 매우 취약한 특성을 가진다. 네트워크카메라를 원격지에 단일 설치함으로써 일반적인 네트워크에 보편화된 침입 탐지 및 차단 시스템의 적용이 불가능하며 보안채널 등의 구성을 위한 네트워크 보안 기술과 암호화 기술 적용이 현실적으로 불가능하고, 다중 사용자와 사용자 별 서비스 품질 차별화 등의 구현에 제약이 많다. 또한 네트워크카메라의 구조적 모순으로 인하여 다중의 네트워크카메라에 대한 효율적인 관리와 사용자별 접근권한 제어가 불가능하다는 단점이 따른다. 특히 네트워크카메라가 이기종일 경우에는 기종간 호환성문제가 있기 때문에 더욱 더 관리가 힘들어질 뿐 아니라 영상 서비스에도 심각한 영향을 미칠 수 있으므로 이기종간 통합 문제가 심각한 실정이며 이를 해결하기 위한 연구가 진행중에 있다.[1]

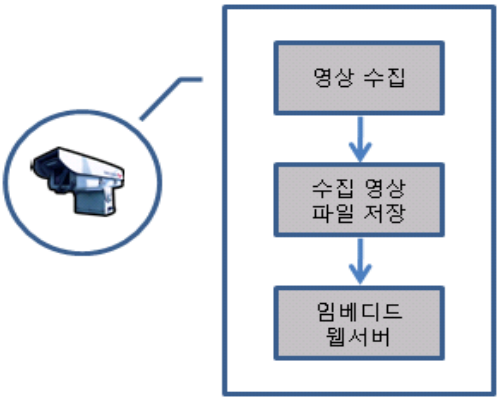
따라서 본 논문은 상기한 바와 같은 보안에 취약한 기존의 네트워크카메라에 대하여 임의의 접속을 시도하는 클라이언트로부터 접속정보를 은닉하고 검증된 클라이언트만의 접속을 지원하며 영상정보에 대한 등급의 설정과 등급별 클라이언트에 대한 차별화 서비스를 제공하는 보안 프락시 서버의 구조를 제안하고 이를 설계 및 구현하였으며 실험을 통하여 프락시 서버가 네트워크카메라의 보안 특성을 개선하면서도 네트워크카메라에 직접 접속하는 경우에 비교하여 서비스 품질이 동등한 수준으로 유지됨을 검증하였다.

본 논문의 구성은 다음과 같다. 2장에서 현재 설치되어 사용되고 있는 네트워크카메라의 설치 현황에 대한 통계를 서술하였고 3장에서는 프락시 서버에서 네트워크카메라와 클라이언트에 대응하기 위한 기술을 설명한다. 4장에서는 구현한 서버의 실험 결과를 나타내고 5장에서 결론을 서술한다.

2. 네트워크카메라의 취약점 분석

네트워크카메라를 구성하는 주요한 요소 기능들을 분류하면 자연 영상을 수집하여 압축하기 위한 영상 수집부와 수집한 압축 영상정보를 파일로 저장하는 파일 관리부, 서비스 클라이언트에게 해당 영상정보를 제공하기 위한 웹서버로 나누어 볼 수 있다.

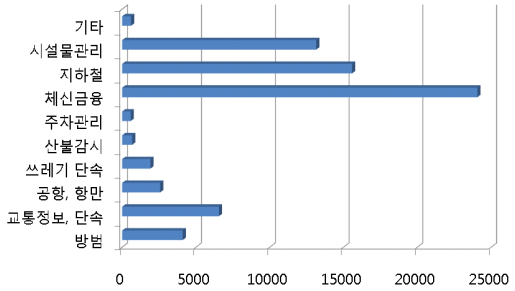
상기의 요소 기능 중에서 웹서버는 서비스 클라이언트와의 정보 교환에 있어서 가장 중요한 부분으로 클라이언트에 대한 접속 인증 및 관리 기능을 포함한다.



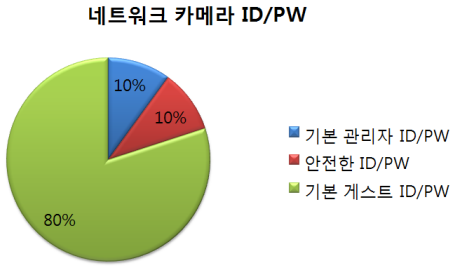
(그림 1) 네트워크 카메라 구성

네트워크 카메라 내의 웹서버에 의한 접속 인증은 일반적인 웹서버의 인증과 동일한 수준으로서 클라이언트 ID와 패스워드를 이용하여 클라이언트를 인증한다. 따라서 네트워크카메라의 보안 문제는 클라이언트의 ID 및 패스워드의 관리 문제와 직결된다. 현재 국내 지자체에서 각 지역별로 설치된 카메라의 수는 정확한 통계는 없으나 대략 6만 9천대에 이를 것으로 추정되며 (그림 2)에 카메라의 용도에 따른 분포상황을 보인다.[4]

이러한 네트워크 카메라는 설치시기와 장소, 생산자 등이 다양하고 일관된 관리 정책이 부재한 상태에서 설치됨으로써 그 관리 체계가 불안하며 이에 따라 각 네트워크 카메라별 접속 정보



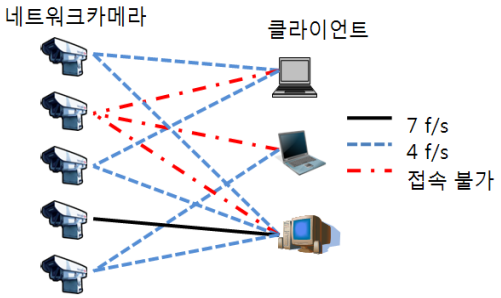
(그림 2) 카메라 설치 현황



(그림 3) 네트워크 카메라에 설정된 인증 정보(ID/PW) 통계

나 접속 권한에 대한 보안 수준이 매우 취약하여 지자체에서 설치한 많은 교통 카메라 및 환경 감시 카메라의 접속 정보가 약간의 시간과 노력으로도 일반인에 의하여 쉽게 노출될 수 있다. 일례로 본 연구와 관련한 정보수집 과정에서 다수의 지자체 카메라가 임의로 노출되었으며 특히 접속 정보를 토대로 접속 시도한 결과, 다수의 네트워크 카메라가 인증 절차가 부재하거나 절차가 있더라도 기본 ID 및 패스워드로 설정된 채 인증 절차를 수행하고 있는 것을 발견할 수 있었다. (그림 3)은 한 지자체의 도로 교통 상황 감시 및 하수 종말 처리장 환경 감시를 위하여 설치된 네트워크카메라 96대의 ID와 패스워드 설정 통계를 나타낸 것으로 안전한 ID와 패스워드로 설정된 네트워크 카메라는 10% 수준이고 기본 ID와 패스워드로 설정되어 있는 카메라가 90% 수준임을 보이고 있다.

과거 CCTV(Closed-Circuit Television)로서 폐쇄된 환경에서 배타적 접속용으로 사용되었던 카메라들이 네트워크와 연동되면서 정책의 부재로 인하여 허가된 클라이언트만이 아닌 일반인도 네트워크카메라가 사용하는 IP와 포트 정보 그리고 기본 ID와 패스워드만을 가지고 대부분의 영상을 볼 수 있다. 또한 카메라의 생산자와 종류가 다양하고 각 카메라마다 개별 관리되며 관리하는 단체가 서로 다르기 때문에 통합적 관리가 어렵다. 또한 (그림 4)에서와 같이 현재 사용되고 있는 네트워크카메라에 접속을 요청하는 경우 클라이언



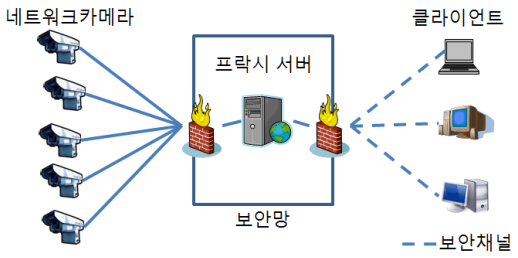
(그림 4) 클라이언트 접속에 따른 서비스 품질

트 수가 증가할수록 프레임률이 저하되어 서비스의 품질이 떨어질 뿐 아니라 심한 경우 네트워크 카메라에 대한 서비스 거부 공격으로 이어질 수 있다.[5,6]

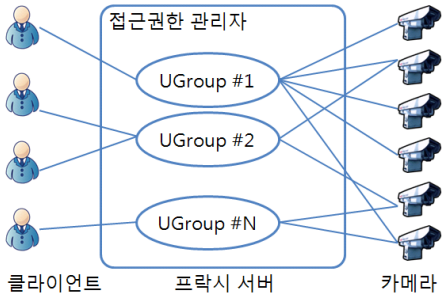
3. 네트워크카메라를 위한 보안 프락시 서버

제2장에서의 네트워크카메라가 가지는 문제점을 해결하기 위해서는 (그림 5)에서와 같이 외부의 침입으로부터 보호받고 있는 안전한 망 내에 위치하는 프락시 서버를 두고 네트워크카메라의 영상정보를 요청하는 클라이언트의 모든 접속이 보안채널을 제공하는 프락시 서버를 통하여 이루어지도록 함으로써 네트워크카메라로의 악의적인 임의접근을 차단해야 한다.

상기의 프락시 서버는 기존에 설치된 카메라의 환경설정 정보가 클라이언트에게 직접 노출되지



(그림 5) 프락시 서버 배치

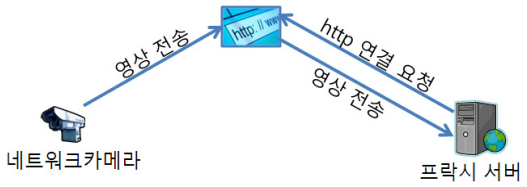


(그림 6) 접근권한 관리 개선 구조

않으면서도 안전한 클라이언트 인증을 제공하고, 클라이언트별 접근 권한에 따른 차별화된 서비스가 가능하여야 한다. 프락시 서버는 네트워크카메라에 접속하기 위하여 필요한 접속 정보를 은닉하고 영상의 불필요한 유출을 줄이며 클라이언트의 권한에 따른 영상 서비스 품질을 제어하기 위하여 네트워크카메라를 대신하여 클라이언트로부터의 접속요청을 처리할 것이 요구된다. 또한 네트워크 카메라와의 단일 접속만을 유지함으로써 서비스 거부 공격으로부터 네트워크카메라를 보호하고 서비스를 위한 영상의 종류를 클라이언트의 접근 권한에 따라 구분함으로써 영상정보에 대한 무분별한 접근을 차단해야 한다. 기존의 개별적 관리 대상이 되었던 네트워크카메라 구조의 취약사항 및 이에 대응하여 제시하는 프락시 기반 서버 구조에서의 개선 방안을 정리하면 [표 1]과 같다. (그림 6)은 프락시 서버에 접속하는 다중 클라이언트를 대상으로 네트워크카메라 영상을 접근권한별 그룹으로 지정하여 접근제어가 가능한 클라이언트 관리 구조의 개선 방안을 나타내었다. 본 장에서는 이러한 프락시 서버가 제공해야 할 역할을 정의하고 이를 위한 구성요소별 세부구조 및 프락시 서버와 클라이언트간의 프로토콜을 제안한다.

(표 1) 기존 방식 대비 프락시 서버 방식에서의 개선사항

항 목	기존 개별 카메라 기반 방식의 취약점	제안하는 프락시 서버 방식의 해결방안
관리정책	설치시기, 장소, 생산자 등에 대한 일관된 관리정책 부재	서버의 관리자 모드에서 모든 등록된 카메라를 일관적으로 관리
정보변경	개별적 관리방식에 따라 총체적 인증정보변경 등 보안정책 적용 곤란	통합된 서버에서 인증정보 변경 및 보안정책 제어
접근권한	접근권한을 획일적인 관리자 인증정보만으로 해결	카메라 및 클라이언트 그룹별 차별화된 다중 접근권한 제공
접속정보	접속을 위하여 각 카메라에 대한 접속정보 및 인증정보 공개 필요	카메라 인증정보를 은닉하고 서버에 등록된 사용자 접근권한 및 인증정보 활용
접근차단	보안망과 격리된 원격에 설치되어 무작위 접속 시도 가능	방화벽 등에 의해 보호되는 보안망 내에 서버를 설치하여 보안성 증대
다중접속	성능 상 접속가능 클라이언트 수 제한으로 다중 접속 불가	다중 클라이언트 접속의 원활한 지원으로 대국민 서비스 가능
관리연계	기관 및 부처 간의 관리에 대한 연계 기능이 부재하여 상호 통합 불가	서버 간의 캐스케이드 증설 방식으로 기관 및 부처 간의 영상정보 교환



(그림 8) 영상 수집 과정

3.1 네트워크 카메라 영상 수집

네트워크카메라에서 영상을 서비스하기 위한 방법으로는 디지털 변환하여 수집한 영상을 JPEG 형식으로 인코딩한 후 파일을 생성하여 저장하고 생성한 파일을 임베디드 웹서버에 게시하여 서비스한다.[2] 클라이언트는 임베디드 웹서버로의 접속정보를 토대로 네트워크카메라가 게시한 파일을 요청함으로써 해당 영상정보를 제공받는다. 그러나 제3장에서 기술한 프락시 서버를 이용하여 보안을 강화하는 경우 네트워크카메라는 프락시 서버와의 접속만을 유지하고 연결된 네트워크카메라의 서비스를 이용하기 위한 요청은 프락시 서버에서 처리한다. 전술한 바와 같이 네트워크카메라는 웹서버를 통하여 영상파일을 제공하고 있으므로 네트워크카메라에 접속하여 영상을 수집하기 위해서는 HTTP(Hyper Text Transfer Protocol) 메시지를 이용할 수 있다.[3,7,8]

HTTP 메시지를 이용하여 네트워크카메라의 영상을 요청하는 경우 프락시 서버는 클라이언트를 대신하여 네트워크카메라로의 접속 정보를 유지 및 관리한다. 프락시 서버로부터 요청 메시지를 수신한 네트워크카메라는 메시지 내부에 포함되어 있는 접속 정보를 이용하여 프락시 서버를 인증하고 해당 영상을 프락시 서버로 전송한다. (그림 7)은 프락시 서버가 네트워크카메라로부터 영상을 수신하는 과정을 나타내었다.

프락시 서버는 네트워크카메라에 접속을 유지하기 위해 네트워크카메라의 아이피와 포트번호가 필요하며 프락시 서버가 네트워크카메라에 인증과정을 통과하고 네트워크카메라에 접속하기 위해서는 네트워크카메라에서 사용자 인증을 위해서 사용되는 ID와 패스워드 정보가 필요하다. 또한 네트워크카메라의 종류에 따라서 인증에 사용하는 ID와 패스워드의 디코딩 방식이 다르고 수집영상을 압축하기 위한 방식이 다양하므로 네트워크카메라의 종류에 따라 디코딩 방식을 구분하여 저장하기 위한 필드가 필요하다. 그리고 네트워크카메라가 설치된 위치에 따라서 같은 시나도 단위로 관리가 가능하도록 인접한 네트워크카메라들을 하나의 그룹으로 지정함으로써 다수의 네트워크카메라에 대한 편의성을 제공할 수 있다. 상기의 정보들을 기반으로 네트워크카메라와 통신하고 관리에 필요한 정보들을 프락시 서버에서 관리함으로써 네트워크카메라에 대한 접속정보의 은닉이 가능하고 네트워크카메라의 관리가 독립적으로 이루어지며, 다양한 네트워크카메라의 통합관리가 가능하다. (표 2)는 네트워크카메라의 관리에 필요한 접속정보를 나타내었다.

(표 2) 네트워크카메라의 접속정보

접속 정보	설 명
camera_id	네트워크카메라의 위치와 이름
user_id	네트워크카메라의 접속 ID
ip	네트워크카메라의 접속 아이피
compression	영상 압축 형식
group	네트워크카메라가 속한 그룹
type	네트워크카메라의 종류
password	네트워크카메라의 접속 비밀번호
port	네트워크카메라의 포트번호
channel	네트워크카메라의 채널
use_camera	네트워크카메라의 활성화 여부

3.2 클라이언트 제어 프로토콜

네트워크카메라로부터 해당 영상을 취합한 프락시 서버는 클라이언트의 권한에 따라 영상을 구분하여 서비스하고 클라이언트와의 올바른 통신과 오류에 대응하기 위하여 클라이언트의 정보와 클라이언트를 제어하기 위한 프로토콜의 정의

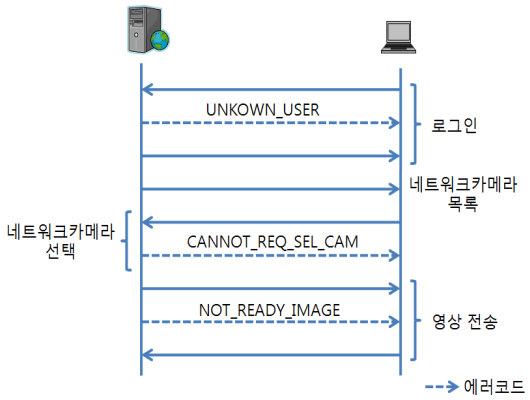
(표 3) 클라이언트 정보

클라이언트 정보	설 명
ip	클라이언트의 아이피
port	클라이언트의 포트
client_id	클라이언트의 ID
client_password	클라이언트의 비밀번호
camera_group	선택한 카메라가 속한 그룹
select_camera	카메라 선택
camera_ch	선택한 카메라의 채널
camera_type	선택한 카메라의 종류
camera_format	선택한 카메라의 영상 압축 방법
image_time	영상의 타임스탬프

가 필요하다. 우선 클라이언트의 관리하기 위해서 프락시 서버에 등록되어야하는 정보로는 다음과 같다. 프락시 서버에서 취합하고 관리하는 영상들에 대하여 클라이언트의 무분별한 접근과 유출을 방지하기 위하여 접근권한을 판단하기 위한 기준이 마련되어야 하며 그 기준은 프락시 서버에 등록된 클라이언트의 ID와 패스워드를 기반으로 생성되어질 수 있다. 클라이언트를 인증한 후 접근권한에 따라 영상을 서비스하는 동안 네트워크카메라에서 프락시 서버로 전송되는 이미지의 속도와 클라이언트에서 프락시 서버로의 영상 요청 속도에 차이가 있을 경우 클라이언트에서 이미지 역전현상이 나타날 수 있다. 이러한 이미지 역전현상을 방지하기 위해서는 영상에 대한 순서가 유지되어야 하며 프락시 서버에서는 순서의 유지를 위하여 네트워크카메라로부터 영상을 받은 시점에 타임스탬프를 영상과 함께 관리하는 방법을 사용할 수 있다. 상기의 정보를 기반으로 영상 서비스가 가능한 클라이언트를 프락시 서버에 등록하고 클라이언트는 영상 서비스를 요청하기 위하여 프락시 서버로 접속함으로써 클라이언트가 네트워크카메라에 별도로 접근하지 않고 영상 서비스를 이용할 수 있어 네트워크카메라에 대한 접속 정보의 은닉이 가능하며 데이터베이스와 연동하여 네트워크카메라의 통합적 관리가 용이하다. 프락시 서버에서 클라이언트의 관리를 위하여 사용하는 정보는 (표 3)과 같고 해당 정보는 프락시 서버로 접속하여 인증 과정을 거친 후 권한별 서비스 품질을 결정하는데 중요한 요소이다.

프락시 서버에서 영상을 서비스하기 위해 사용하는 프로토콜에서 필요한 과정은 다음과 같다. 클라이언트는 프락시 서버에서 제공하는 영상 서비스를 이용하기 위해서는 프락시 서버에서 클라이언트 인증 과정 거쳐 접속을 요청하는 클라이언트의 정당함을 검증하는 과정이 선행되어야 하므로 프락시 서버에 등록된 클라이언트의 ID와 패스워드를 포함한 요청 메시지를 생성하여 프락시 서버로 전송함으로써 클라이언트의 검증이 가능하다. 또한 프락시 서버는 클라이언트 인증 후 클라이언트의 접근권한을 결정하여 서비스 가능한 네트워크카메라의 영상을 구분하는 기준으로 ID와 패스워드를 사용한다. 상기의 과정을 수행함으로써 프락시 서버와 클라이언트에서 영상을 서비스하기 위한 세션을 성립할 수 있다.

클라이언트에서는 네트워크카메라의 영상을 서비스 받기 위하여 접근이 허가된 네트워크 카메라의 목록이 필요하여 프락시 서버는 등록되어 있는 네트워크카메라들 중에서 영상을 요청하는 클라이언트에게 접근이 허가된 네트워크카메라의 목록을 색인화하여 클라이언트에게 전달하기 위한 과정이 요구된다. 클라이언트는 색인화한 네트워크카메라의 목록을 선택하여 프락시 서버로부터 해당 네트워크카메라의 영상을 요청함으로써 네트워크카메라의 영상을 수신할 수 있다. 또한 프락시 서버와 클라이언트의 영상 전송 과정 중에 네트워크의 대역폭 손실과 프락시 서버의 부하를 줄이기 위하여 프락시 서버에 영상이 준비되지 않았을 경우 네트워크카메라에서 영상을 수신하는 속도와 클라이언트로 영상을 수신하는 속도를 균형있게 유지할 필요가 있다. 이에 프락시 서버에서 클라이언트로 전송할 영상이 준비되어 있지 않을 경우 영상의 원활한 서비스를 제공하기 위하여 일정한 유휴시간이 필요하다. (표 4)는 클라이언트와의 통신 과정을 제어하기 위해서 각



(그림 8) 프락시 서버와 클라이언트 통신 과정

과정에서 이용되는 명령들을 정의하였고, (그림 8)은 클라이언트가 네트워크카메라의 영상을 수신하기 위해서 프락시 서버로 접속하여 영상을 요청하는 과정을 나타내었다.

프락시 서버와 클라이언트가 기 정의한 프로토콜을 사용하여 통신하는 과정 중에 다수의 클라이언트를 처리하는 프락시 서버는 정당하지 않은 클라이언트의 접근과 프락시 서버의 이상으로 인하여 원활한 서비스를 제공하지 못할 경우에 대비하여 클라이언트에게 프락시 서버의 상태명령을 전달함으로써 클라이언트에서 서비스의 장애요인을 판단할 수 있다. 프락시 서버의 상태명령으로는 클라이언트가 인증을 요청하였을 경우 ID와 패스워드가 일치하지 않으면 인증이 불가능함을 나타내는 상태명령이 사용되고, 프락시 서버와 클라이언트의 통신에 사용되는 프로토콜을 일치시키기 위한 상태명령이 필요하다. 또한 클라이언트가 프락시 서버의 허용 범위를 초과 접속한 경우 클라이언트가 다른 프락시 서버에 접속할 수 있도록 하기 위한 상태코드가 필요하다. (표 4)는 프락시 서버의 상태를 위한 명령을 나타내었고, 프락시 서버는 상태 명령을 이용하여 인증되지 않은 클라이언트의 접속을 차단하고 영상을 서비스하는 과정에서 일어나는 프락시 서버의 상태를 클라이언트에서 판단할 수 있도록 정보를 제공한다.

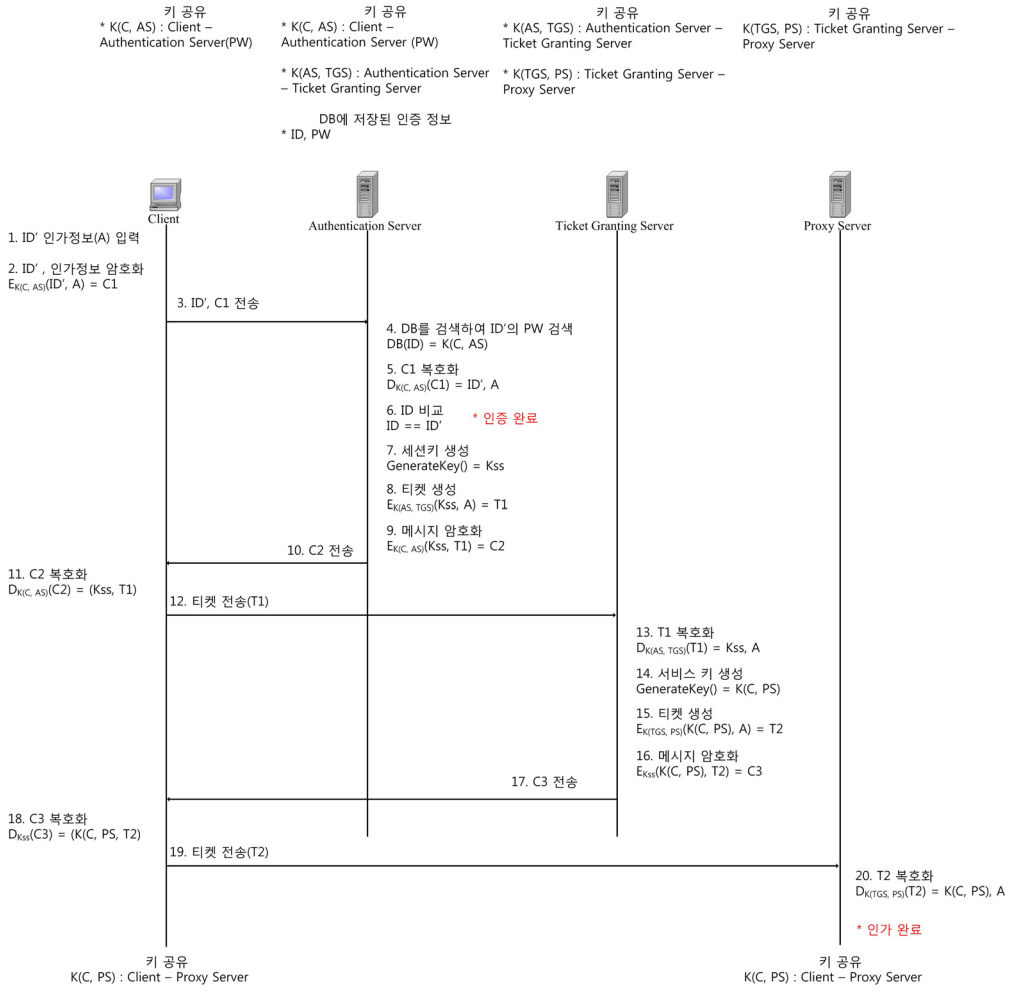
(표 4) 프로토콜 정의

프로토콜 명령어	설 명
REQ_CONNECT	서버와의 연결 요청
RES_CONNECT	서버와의 연결 요청 응답
REQ_SEL_CAM	감시 시스템 선택 요청
RES_SEL_CAM	감시 시스템 선택 응답
REQ_IMAGE	영상 전송 요청
RES_IMAGE	영상 전송 응답
REQ_DISCONNECT	서버와의 연결 해제 요청
RES_DISCONNECT	서버와의 연결 해제 응답
RES_ERROR	에러

3.3 사용자 인증, 인가 및 세션키 분배 프로토콜

상기한 클라이언트의 사용자 인증과 등급별 서비스를 위한 인가는 보안채널을 이용하여 통신하여야 한다. 따라서 본 논문에서는 클라이언트의 사용자 인증, 인가를 위해 커버로스 인증 프로토콜을 활용하였으며, 커버로스 내에서 인증에 사용되는 티켓을 추가하여 사용자 인가를 제공한다. 이에 대한 프로토콜은 (그림 9)와 같다.

1. 클라이언트는 인증, 인가를 위해 ID'와 인가정보(A)를 입력한다.
2. 입력된 인증, 인가 정보(A)를 클라이언트와 인증 서버간 사전에 공유된 키(패스워드, K(C, AS))를 기반으로 암호화한다.
3. 사용자로부터 입력받은 ID'와 암호화된 인증 정보(C1)을 인증 서버로 전송한다.
4. 인증 서버는 수신한 ID'를 이용하여 DB에 저장된 키를 검색한다.
5. 검색된 키(K(C, AS))를 기반으로 수신한 C1을 복호화하여 ID'과 인가정보(A)를 추출한다.
6. 복호화된 ID'과 ID를 비교하여 올바른 사용자인지 확인한다. 이 과정이 인증 과정이다.
7. 클라이언트와 티켓 그랜팅 서버간 통신을 위한 세션키(Kss)를 생성한다.
8. 생성된 세션키(Kss)와 인가 정보(A)를 인증 서버와 티켓 그랜팅 서버간 공유된 키(K(AS,



(그림 9) 사용자 인증, 인가 및 키 분배를 위한 보안 프로토콜

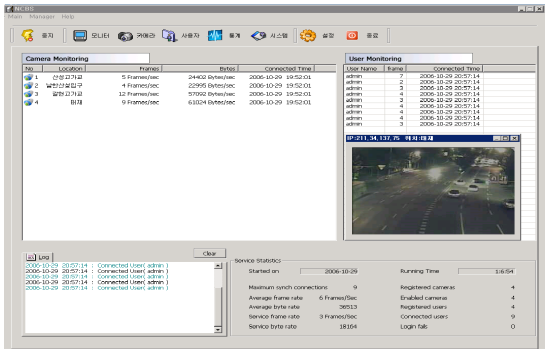
TGS))를 기반으로 암호화하여 티켓(T1)을 생성한다.

9. 생성된 세션키(Kss)와 티켓(T1)을 클라이언트와 인증 서버간 공유된 키(K(C, AS))를 기반으로 암호화(C2)한다.
10. 클라이언트로 C2를 전송한다.
11. 클라이언트는 수신한 C2를 클라이언트와 인증 서버간 공유된 키(K(C, AS))를 기반으로 복호화하여 세션키(Tss)와 티켓(T1)을 추출한다.
12. 추출된 티켓(T1)을 티켓 그랜팅 서버로 전송한다.
13. 티켓 그랜팅 서버는 클라이언트로부터 전송된 티켓(T1)을 수신하고 인증 서버와 티켓 그랜팅 서버간 공유된 키((K(AS, TGS))를 기반으로 이를 복호화하여 세션키(Tss)와 인가정보(A)를 추출한다.
14. 프락시 서버의 서비스를 인가하기 위한 서비스 키(K(C, PS))를 생성한다.
15. 생성된 서비스 키(K(C, PS))와 추출된 인가정보(A)를 티켓 그랜팅 서버와 프락시 서버간 공유된 키(K(TGS, PS))를 기반으로 암호화하여 티켓(T2)을 생성한다.

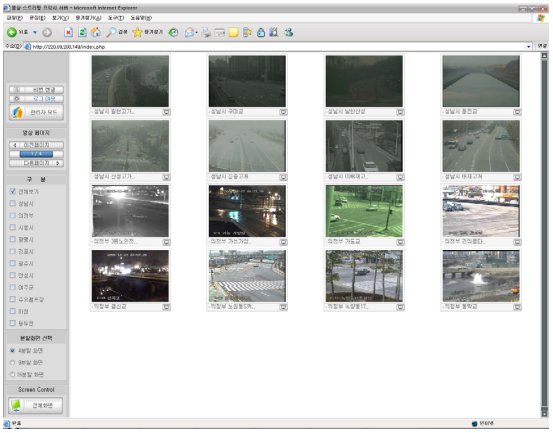
16. 생성된 서비스 키(K(C, PS))와 티켓(T2)을 세션키로 암호화(C3)한다.
17. 클라이언트로 C3를 전송한다.
18. 클라이언트는 C3를 수신하며 세션키(Tss)를 이용하여 C3를 복호화하여 서비스 키(K(C, PS))와 티켓(T2)를 추출한다.
19. 프락시 서버로 티켓(T2)를 전송한다.
20. 프락시 서버는 클라이언트로부터 수신한 티켓(T2)를 복호화하여 서비스 키(K(C, PS))와 인가 정보(A)를 확인한다. 이 과정이 인가과정이다.
21. 상기의 과정이 모두 정상적으로 완료되면 프락시 서버는 요구한 클라이언트의 등급별 서비스를 제공하며, 클라이언트와의 차후 서비스는 공유된 키(K(C, PS))를 이용하여 안전한 채널을 통해 통신한다.

4. 구현 및 결과

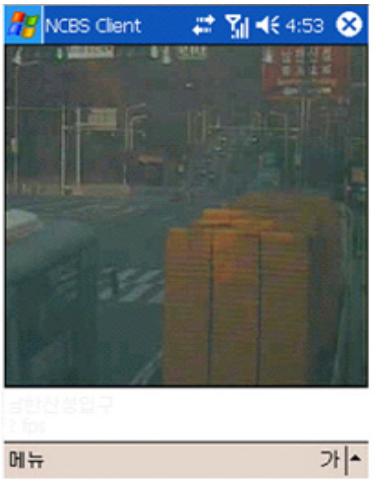
본 논문에서 제안한 프락시 서버는 네트워크카메라와 클라이언트의 관리를 위한 인터페이스를 제공하며 그 구성과 실행 결과는 (그림 10)과 같다. (그림 11)과 (그림 12)는 제 3 장에서 정의한 프로토콜을 이용하여 클라이언트가 사용하는 웹 브라우저의 ActiveX와 PDA를 인증하고 ID와 패스워드를 통한 접근 권한에 따라서 서비스가 가능한 영상들을 분류하여 클라이언트에서 영상을 디코딩한 결과를 나타내었다. (그림 13)은 클라이언트가 네트워크카메라에 직접 접속하여 영상을 수신하는 경우와 프락시 서버를 거쳐 영상을 수신하는 경우 한 프레임 당 지연시간을 나타낸 결과이다. 가로축은 수신된 영상의 프레임 수를 나타내며 세로축은 지연된 시간을 ms 단위로 나타내었다. 네트워크카메라로의 직접접속 지연시간은 평균 42.35ms이고, 프락시 서버를 통해서 접속한 경우 평균 지연시간은 47.525ms로써 평균 5.1ms의 차이가 있음을 확인하였다. 이는 프락시 서버가 네트워크카메라의 접속을 대행하기에 우수한 성능임을 입증한다.



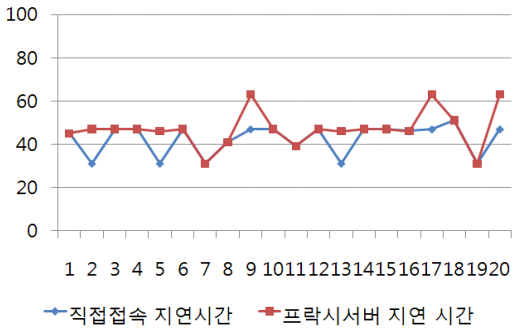
(그림 10) 구현된 서버



(그림 11) 다중 클라이언트 접속



(그림 12) PDA용 클라이언트 접속



(그림 13) 영상 서비스 지연 시간

5. 결 론

최근 교통 상황 감시, 범죄 예방 등의 용도로 네트워크카메라의 사용량이 증가함으로써 개인 정보와 다양한 상황 정보를 갖는 영상의 안전한 관리와 네트워크카메라에 접근 제어와 많은 수의 네트워크카메라를 관리하기 위한 방안이 필요하다. 이에, 본 논문에서는 네트워크카메라와 영상의 관리와 보안을 강화하기 위한 프락시 서버를 구현하였다. 제안한 프락시 서버는 네트워크카메라의 접속 정보를 은닉하고 네트워크카메라에 접속하기 위하여 사용하는 ID와 패스워드를 프락시 서버에서 관리함으로써 서로 다른 네트워크카메라들에 대한 통합적인 관리가 가능하며, 클라이언트의 그룹별 등급에 따라 서비스 영상의 차별화가 가능함을 보였다. 또한, 프락시 서버에 저장된 네트워크카메라의 영상을 안전하게 보호하고 관리하기 위해서 안전하게 보호된 망 내에 프락시 서버를 위치시켜 외부의 불법적인 접근을 제한함으로써 영상 정보의 유출 방지가 가능하며 네트워크카메라에 대한 클라이언트 접근을 프락시 서버가 대행함으로써 네트워크카메라의 접속정보의 은닉이 가능함을 보였다. 마지막으로 서비스 영상 지연시간을 실험하고 분석함으로써 프락시 서버로서의 성능을 검증하였다.

향후 지자체에서 사용하는 네트워크카메라의 통신 프로토콜을 표준화하는 방안이 필요하다고 사료된다.

참 고 문 헌

[1] 임강빈, 배광진, 정태영, “이종 영상전송장치 및 다중다용자 지원을 위한 보안영상 통합분배시스템 개발”, 중소기업청 산학연공동기술개발컨소시엄사업 최종보고서, 2007년 7월 - 2008년 6월

[2] Ikebe, Oqawa, Hatayama, “Network camera system using new home network architecture with flexible scalability”, International conference on ICCE2005, pp. 151-152, Jan. 8, 2005

[3] Y. Hagiwara, T. Furuya, T. Sakurada, and T. Saito, “Surveillance Camera System with a Wired and Wireless Network”, Proceedings of IMSA2005, Hawaii, USA, Aug. 8, 2005

[4] “공공용 CCTV의 설치현황”, 전자신문, Feb. 23, 2008

[5] 곽후근, 정규식, “무선 인터넷 프록시 서버”, 한국컴퓨터종합학술대회 논문집, Vol.32, No.1 (A), pp.313-315, 2005년

[6] 정태영, 이현희, 임강빈, “영상보안용 웹 카메라의 다중 클라이언트 지원을 위한 스트리밍 서버의 설계 및 구현”, 대한전자공학회 제 4권 제 1호, 2006년

[7] “Network camera developments enable live web imaging”, Axis white paper, Nov. 12, 1999

[8] http://www.axis.com/techsup/cam_servers/dev/activex.htm

◐ 저 자 소 개 ◑

배 광 진(Kwangjin Bae)
2005년 2월 순천향대학교 정보보호학과 졸업
2007년 2월 순천향대학교 정보보호학과 석사
2009년 8월 박사과정 수료
2010년 1월~현재 (주) 기가레인 연구원
관심분야 : 시스템보안, 운영체제보안, 융합보안, 모바일보안
E-mail : kjbae@sch.ac.kr

이 경 률(Kyungroul Lee)
2008년 8월 순천향대학교 정보보호학과 학사졸업
2010년 8월 순천향대학교 정보보호학과 석사졸업
2010년 9월~현재 순천향대학교 정보보호학과 박사과정
관심분야 : 시스템보안, 운영체제보안, 임베디드시스템보안, 모바일보안
E-mail : carpedm@sch.ac.kr

임 강 빈(Kangbin Yim)
1992년 2월 아주대학교 전자공학과 졸업
1994년 2월 아주대학교 전자공학과 석사
2001년 2월 아주대학교 전자공학과 박사
1999년 3월~2000년 2월 (미)아리조나주립대학교 연구원
2003년 3월~현재 순천향대학교 정보보호학과 교수
2005년 3월~현재 한국정보보호학회 이사
2009년 3월~현재 한국인터넷정보학회 이사
관심분야 : 시스템보안, 운영체제보안, 융합보안, 모바일보안, 접근제어
E-mail : yim@sch.ac.kr