Journal of Korea Multimedia Society Vol. 15, No. 1, January 2012(pp. 93-100)

CCTV 보안관제 취약성 및 성능 분석

서태웅[†], 이성렬[††], 배병철[†††], 윤이중[††††], 김창수[†††††]

요 약

최근 공간정보기술의 발달에 따라, 여러 분야에 공간정보 기반의 관제 시스템이 운영 중이거나 추진 중에 있다. 특히 CCTV관제 시스템은 다양한 분야에서 활용되는 대표적인 관제 시스템이다. 그러나 통신 네트워크와 맞물리고 시스템 자체의 규모가 커짐에 따라 보안 취약에 관한 문제가 대두되고 있다. 따라서 본 연구에서는 연구가 진행 중인, 혹은 이미 구축 운영 중인 CCTV 영상관제 시스템에서 발생 가능한 취약점을 분석했다. 또한 CCTV 관제 위치정보에 대한 악의적 변경에 대한 재난/테러 대비를 고려해야 한다. 그래서 현재 운용중인 방범용 CCTV관제 시스템을 실험 대상으로, 악의적인 공격 시뮬레이션을 분석하였다. 또한 이 공격이 관제 운용영역(커버리지)을 감소시켜 어느 정도의 관제 성능이 저하되는지 분석하기 위한, 수식을 작성 했다.

An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control

Tae Woong Seo[†], Sung Ryoul Lee[††], Byung Chul Bae[†††], E-Joong Yoon[††††], Chang Soo Kim[†††††]

ABSTRACT

Recently, the security monitoring and control systems based on spatial information in various field are operated and being developed according to evolve the spatial information technology. Especially, the CCTV monitoring and control system can be used in various field as a typical system. However, the security vulnerability problems have become an issue because the system connected by computer network and getting bigger than before. Therefore we studied security vulnerabilities of CCTV monitoring and control system which is being developed and operated. In addition, it is important to consider disaster and terrorism with unauthorized changes on location information. Therefore we analyzed the performance of observation when the cameras are break down as a result by hacking to CCTV monitoring and control system.

Key words: Security Monitoring and Control(보안관제), CCTV Vulnerability(CCTV 취약성), Performance analysis(성능분석), Disaster Prevention(방재)

※ 교신저자(Corresponding Author) : 김창수, 주소 : 부산광역시 남구 대연 3동 599-1 부경대학교 IT융합응용공학과(608-737), 전화 : 051)629-6245, FAX : 051)629-6230, E-mail : cskim@pknu.ac.kr
접수일 : 2011년 10월 24일, 수정일 : 2011년 12월 27일
완료일 : 2012년 1월 11일
[†] 준회원, 부경대학교 IT융합응용공학과 석사과정
(E-mail : efisode@pknu.ac.kr)
[††] 정회원, ETRI 부설연구소
(회사 정책상 비공개 요청)
[†††] 정회원, ETRI 부설연구소 과제책임
(회사 정책상 비공개 요청)
[††††] 정회원, ETRI 부설연구소 선임본부장
(회사 정책상 비공개 요청)
[†††††] 종신회원, 부경대학교 IT융합응용공학과 교수

1. 서 론

CCTV 등의 영상관제시스템은 방범기능 외에도 지능형 교통망 체계 (ITS : Intelligent Traffic System)와 연계되거나 소방, 경찰 등과도 밀접한 연관을 가지고 운영되고 있다. 그러나 현재의 CCTV 장치 등은 보안이 매우 취약한 상태에서 관리되고 있기 때문에 악의적인 공격으로 CCTV의 순기능이 운영되지 않을 수 가능성이 있다. 이를 위해서는 반드시 공간정보 기반의 분석기능이 필요하며, 영상장치에 대한 해킹 예방 기술 등에 대한 방법들이 연구되어야 한다[1].

관제시스템의 요소 기술이 발전하고 관제 대상이 확대되는 반면에, 시스템의 구조는 복잡해지고 보안 위험에 쉽게 노출되는 문제점이 발생한다. 특히 국가 기반의 관제 시스템의 경우, 해당 시스템의 동작불능, 오작동, 해킹 등과 같은 문제는 심각한 결과를 초래한다. 그 문제가 국가 안보나 국민의 안전의 문제와 연결되기 때문이다[2].

최근, 'CCTV통합관제센터' 구축으로 경찰이 운용주체가 되어 화상순찰을 실시할 수 있게 되었다. 설치단계에서부터 관련부서와 연계하여 최적의 위치를 선정하여 최첨단 카메라를 설치하였고, 긴급 상황이 발생하면 위치정보를 활용하여 투망형태로 목표물을 따라가며, 그 경로를 추적할 수 있게 된다. 이렇게 통합 관제 시스템은 범죄 시도를 사전에 차단하는 한편, 범죄 발생 시 경찰이 직접 신속하게 대처할 수 있다는 것이 장점이다. 이러한 통합관제센터는 천안·아산지역을 시작으로, 여러 지자체에서 기존 관제센터에 추가적으로 GIS기반의 신기술을 적용·확장하여 운용 중이다.

그러나 CCTV 통합 시스템이 구축이 완료 되면, 그 규모가 시 단위나 국가적인 규모로 확대될 수 있고 이를 관리하기 위한 네트워크 또한 거대해진다. 이러한 네트워크에 악의적인 접근 및 공격이 가해지면 그 피해는 매우 심각해진다. 또한 CCTV 카메라가 실외에 설치되기 때문에 보안적인 문제와 함께 주위 환경에 따른 물리적 손상의 위험도 고려해야 한다. 이때는 CCTV 촬영 대상에 대한 관제의 개념과, CCTV 시스템 자체에 대한 상태 모니터링과 제어가 포함된, 시스템 스스로에 대한 보안 관제의 필요성이 증가한다고 볼 수 있다.

CCTV 관제 시스템의 주요 보안상의 문제점들을 다음과 같이 정리 할 수 있다[3].

- 옥외에 설치된 CCTV 카메라와 케이블의 물리적 보안 취약문제
- 녹화된 CCTV 영상의 프라이버시 문제
- CCTV 관제 센터로의 침투 경로로 악용될 가능성
- 특정 인터넷 검색엔진에 노출된 네트워크 기반 CCTV의 IP 공개
- CCTV 네트워크 장비, 관리 프로그램의 보안 취약성

2. 관련연구

2.1 보안관제

기존의 관제의 기능은 일반적으로 국가 기관의 보안 업무를 위한 감시활동이나, 공항 등의 큰 규모의 체계에서 항공기의 비행 통제와 모니터링 및 제어 활동을 의미한다. 특히 비행통제의 경우 제어명령을 통해 기계장치를 제어하고, 다수의 장비에 상황을 모니터링 하는 복잡한 과정을 거치게 되는데 이러한 일련의 활동을 관제라고 칭하고 있다. 업무 현장의 감시, 감독의 'Supervision'라는 의미나, 물류 등의 이동 상황을 'Monitoring and Control' 한다는 의미로도 볼 수 있다. 즉 관제라는 의미는 의 두 가지 기능이 복합적으로 적용된 의미로써 한다는 의미로 볼 수 있다.

본 연구에서 말하는 '관제'라는 의미는 광범위하게 사용되고 있는 현재 실정에 맞춘 것이다. 즉 전산망 보급이 확대되어 흔히 사용되는 'Monitoring'의 의미는 '컴퓨터 프로그램의 수행 중에 발생 하는 오류에 대비한 감시 활동', '국가나 공항 따위에서 필요에 따라 강제적으로 관리하여 통제하는 일'을 의미하여 그 의미가 아주 제한적이다. 따라서 최근 연구되고 있는 다양한 분야의 융합기술의 경계가 모호해짐에 따라 기존 관제의 개념을 확장할 필요성이 커졌다[4]. 또한 전산망 보급이 확대 되면서 '보안관제'라는 용어의 정의가 필요하게 되었다. 미국의 R. Bejtlich는 전산망 보안 관제란 '네트워크 트래픽을 분석하고, 침입자의 공격을 규명하는 등의 행위'라고 규명하였다[5].

2.2 CCTV/영상관제 현황

CCTV통합관제센터는 공공부문의 다양한 CCTV

영상정보를 관리하기 위한 제반자원 및 전담 운영조직 체계인 국가영상정보자원과 관제센터의 하드웨어, 솔루션, 기반시설, 공간구조에 해당하는 시스템을 효율적으로 운영하고 관리하기 위한 시스템 및 운영조직을 말한다. 이는 국가영상정보자원의 효율적 운영・관리를 위한 통합기반 인프라를 제공하고, 기본서비스, 확장서비스, 연계서비스 등의 서비스 업무를 수행한다. 또한 국가영상정보자원 총괄업무(계획수립, 업무분장, 조직운용, 정보보안 등), 운영업무(장애관리, 백업관리, 시설관리 등), 관제업무 등을 추가적으로 수행한다[6].

현재 국내의 CCTV 통합관제센터는 2010년 말을 기준으로 25개소(서울시 12개 구청, 경기도 7개 지자체, 대전광역시 2개구 순)가 운영 중에 있으며, 2011년도에는 부산광역시 4개소를 포함하여 34개 지자체가 통합관제를 구축할 예정이다. 또한 부산정보고속도로의 인프라를 활용한 자가 광대역 통신망으로 빠르고 선명한 영상정보 제공을 목표로 하고 있다.

2010년 9월에는 강원지방경찰청에서 서별로 운영하고 있는 방범용 CCTV를 경찰청으로 통합하여 '차량번호 판독용 CCTV 통합관제 시스템(VICIOS : Vehicle number Identification CCTV Integration Oversee System)'을 구축하였다. 방범용 CCTV의 종류에는 크게 두 가지가 있는데, 일반 방범용 CCTV는 놀이터, 공원 등 우범지역에 설치되어 차량번호 촬영기능 없이 동영상만을 촬영하는 장비이며, 차량번호 판독용 CCTV는 도로위에 설치되어 통과 차량을 촬영하여 차량번호를 자동으로 판독하는 장비이다. 강원 경찰청은 이 중에서 차량번호 판독용 CCTV를 192대 설치하고 150여 건의 사건을 해결했다. 이 관제 시스템은 영상을 통합관제실로 전송하여 실시간으로 예상 도주로를 판단하는 시스템으로서, 범행 차량을 확보한 후, 시스템에 입력한 후, 해당 차량이 관제 지역으로 진입하면 VICIOS시스템이 즉시 동작, 알림서비스를 제공한다. 경찰 관할 내의 도주경로를 분석하고 해당 지역을 순찰하여 검거하는 방식이다[7].

한편, 2010년 말 조사에 의하면, 전국 34,241대의 방범용 CCTV가 설치되어 있다. 특히, 서울과 경기도의 합이 약 15,000대에 이르러 절반 가까이 수도권에 집중되어 있었고, 이 중 부산시에는 625대(약 1.8%)의 CCTV가 설치되어 있었다.

부산시의 공공기관 CCTV 네트워크 구성 형태를 보면 동축케이블을 통해 영상을 전송하는 형태가 약 75%를 차지하는데, 현재까지는 과반수의 관제가 아날로그 CCTV 카메라를 사용하고 있다[8]. 다만 앞으로 통합관제센터의 비율과 함께 네트워크 카메라의 비율이 점차 높아질 것으로 예상되며 이에 따른 보안문제를 간과 할 수 없는 실정이다.

3. 영상 관제 시스템의 취약점 분석

영상관제 자체로도 보안 및 개인 프라이버시의 문제를 가지고 있는데다, 최근 CCTV 통합관제가 컴퓨터 네트워크와 맞물리면서 해당 보안 문제점을 그대로 안고 있는 상황이다. 그리고 CCTV 통합관제센터의 관리 주체가 국가기관 및 지자체인 것을 감안하면, 악의적인 공격 및 접근을 당했을 때 그 위험의 정도는 심각하다.

CCTV 구성 시스템의 특성상 카메라가 외부에 노출되어있어 악천후 등의 외부 환경에 취약할 뿐만 아니라 악의적인 중앙 시스템으로의 침투로 악용될 수 있다. 정보시스템의 위험 분석을 위해서 표 2과 같이 관리, 물리, 기술적 분류로 나누는데 그 항목의 대부분은 CCTV/영상관제에 있어 필수적인 것들이 많다.

관제 시스템에 있어 CCTV가 해킹/크래킹의 대상이 될 수 있는 보고된 사례와 발생 가능한 해킹 방법을 분석하기 위해, 현재 설치・운영되는 CCTV 시스템 방식에서 발생할 수 있는 보안 위협들은 다음과 같이 세 가지로 구분하였다. 특히 3.1 네트워크 기반의 CCTV 시스템은 기존의 컴퓨터 네트워크 해킹 문제와 결합되어 많은 보안 취약점이 발견되었다.

표 1. 기본적인 위험 분석의 항목[9]

분 류	통 제 항 목
관리적	정책 및 절차, 직원통제, 감독구조, 보안의식 훈련, 시험
물리적	네트워크분리, 경계선보안, 컴퓨터통제, 직업영역구분, 데이터백업, 케이블링
기술적	시스템접근, 네트워크구조, 네트워크접근, 암호화, 프로토콜, 통제구역, 감사

3.1 네트워크 기반의 CCTV 시스템에서 발생하는 보안 위협

공인 IP를 이용하는 CCTV 시스템의 경우, 다양한

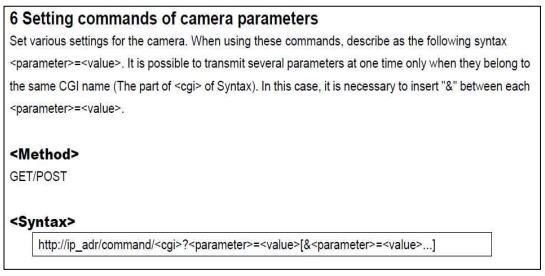
경로를 통해 IP주소의 노출에 대한 우려이다. 이렇게 습득된 IP주소는 여러 가지 크래킹 소프트웨어를 이용해 CCTV 시스템에서 사용하는 관리자 ID와 패스워드를 찾아내어 무단으로 영상 정보를 보거나 습득할 수 있다.

특히, 최근 해커들은 '구글(Google)' 검색 엔진을 악용하여 해킹을 시도하고 있는데, 구글은 1만여 개의 구글 서버에 2주일에 한 차례씩 전 세계 30억여 개의 웹 사이트 및 서버를 검색하여 갱신되는 정보를 구글 컴퓨터에 복사하고 검색 엔진으로 제공하고 있어 타 검색 엔진보다 방대한 량의 정보를 보유하게 된다[10]. IP를 가지고 인터넷에 연결하여 영상 정보를 전송하는 CCTV, 네트워크 카메라 및 웹캠 역시 이 보안성 취약점에 노출되어 구글 검색 엔진을 통해 해킹되어 그 영상이 노출되어 문제가 되고 있다.

이와 더불어 URL 분석을 이용한 공격 방법을 들 수 있다. 그림 1의 매뉴얼은 'SONY' 사의 'CGI Command Manual'의 일부인 "6 Setting Commands of camera parameters"에 대한 설명이다. IP 기반 카메라는 해당 Web Site 주소를 통해 매뉴얼에 명시된 Parameter와 해당 Value 값을 URL에 작성한 후 링크를 통해 카메라를 컨트롤 할 수 있게 된다.

단, 제조회사마다 파라미터나 디렉터리는 다르지만, 제공되는 웹 기반의 관리 어플리케이션을 통해서 제조사를 알아 낼 수 있으며, 특히 영상 뷰어 기능을 위해 설치되는 ActiveX의 배포자를 통해서도 확인할 수 있다. 제조사를 알게 되면, 인터넷 검색을 통해 카메라의 스펙, 상세 매뉴얼, 조작 방법 등을 찾는 것은 어렵지 않다.

표 2는 구글 검색 엔진을 이용하여 CCTV 해킹이 가능한 검색어를 CCTV 종류별로 정리한 것이다. 이 표에서 제시한 검색어로 구글 검색을 통해 검색할 경우 노출된 CCTV의 IP주소를 포함한 URL이 검색


6 Setting commands of camera parameters

Set various settings for the camera. When using these commands, describe as the following syntax <parameter>=<value>. It is possible to transmit several parameters at one time only when they belong to the same CGI name (The part of <cgi> of Syntax). In this case, it is necessary to insert "&" between each <parameter>=<value>.

<Method>

GET/POST

<Syntax>

http://ip_adr/command/<cgi>?<parameter>=<value>[&<parameter>=<value>...]

그림 1. 카메라 조작 파라미터

되는데 이것을 이용하면 CCTV에서 사용자 웹 뷰어로 전송되는 영상을 획득 및 컨트롤할 수 있다.

마지막으로 악성코드를 이용한 ARP Spoofing 공격으로 인한 피해, 네트워크 장비의 계정, 암호 등의 관리 소홀로 인한 보안 위협을 사례로 들 수 있다[11].

3.2 아날로그 CCTV 카메라 방식의 시스템에서 발생하는 보안 위협

아날로그 CCTV 카메라 방식의 시스템은 일반적으로 CCTV 카메라와 DVR 서버가 1:1로 동축케이블을 통해 연결되어 있다. 이 경우 악의적인 공격자에 의해 동축케이블의 절단 등으로 인한 영상 정보 송수신을 가로막는 물리적인 보안 위협, 동축케이블의 분배를 통한 CCTV 영상정보의 무단 모니터링과 같은 소프트웨어적인 보안 위협을 수행할 수 있다.

CCTV 보안 관제센터에서는 이러한 보안 위협에 대해 적극적으로 대처하지 못하기 때문에 기밀한 영상에 대한 누락 또는 노출로 인한 심각한 보안 문제가 발생할 수 있다. 또한 기존 CCTV에는 별도의 암호화 및 인증 기능이 없어 비인가 사용자가 '후킹'기법을 이용해 기존 영상을 다른 영상으로 무단 교체하는 것도 가능하다.

3.3 악의적인 공격자에 의한 보안 위협

CCTV 시스템 환경은 관제센터의 관리 서버가 인터넷에 연결된 상태이며, 서버・관제인력 PC 등의 보안관리 취약으로 해킹 및 자료 유출이 가능하다. 또한 CCTV 시스템 내부망(전자정부통합망 등) 연결 시 내부시스템 또는 타 기관 공격 경로로 악용이 가능하다.

악의적인 공격자가 영상 관제 센터로 무단 침입하거나 방문 업체 직원으로 가장하여 자신의 시스템을 통해 CCTV 시스템의 네트워크 망을 스캐닝 할 수 있다. 또한 CCTV 관제 시스템의 장비의 IP 주소와 ID, 패스워드를 알고 있는 설치 담당자에 의한 영상정보 및 관리 정보 무단 방출을 사례로 들 수 있다. 일부 업체에서는 공공기관에 구축한 사실을 다른 고객사 또는 관계자에게 자랑하듯이 시연해 주고 있어 보안 위협에 대한 불감증이 위험한 수준에 이르렀다고 할 수 있다.

표 2. 네트워크 CCTV 접근이 가능한 검색어 정리

CCTV 종류	검 색 어	컨트롤범위
Axis Camera	/view/view.shtml axis	
	"adding live video to one of your own pages a very easy task with an AXIS 2100 Network Camera"	
	"Live view - / - AXIS"	좌/우
	"Your browser has JavaScript turned off.For the user interface to work effectively"	
	indexFrame.html axis	
	"Live web imaging unleashed“	
Cannon Camera	sample/LvAppl/	
MOBOTIX Camera	/control/userimage.html	
JVC Camera	"(c)copyright 1999-2003 VICTOR COMPANY OF JAPAN, LIMITED. All rights reserved" (- finaly I got to know the meaning of the letters in the brand name JVC :)	
	"V.Networks [Motion Picture(Java)"	
	"Control the Pan/Tilt and move to the Preset Position"	
FlexWatch Camera	/app/idxas.html	좌/우/확대/축소
	"Saving & Retrieving Mode"	
Panasonic camera	/ViewerFrame?Mode=Motion	
TOSHIBA cameras	"TOSHIBA Network Camera - User Login"	
Sony camera	/home/homeJ.html	좌/우/확대/축소
webcamXP	"my webcamXP server!"	
	inurl: /view.shtml	
	inurl: ViewerFrame? Mode=	상/하/좌/우
	intitle: liveapplet	
Evo WebCam	intitle: liveapplet inurl: LvAppl	좌/우/확대/축소
	intitle: “EvoCam” inurl: “ webcam.html”	

4. CCTV 관제 시스템의 해킹 상황에 따른 관제 성능 분석

본 연구에서는 앞 절에서 제시한 세 가지 CCTV관제 보안 취약성 중에서, 보안 위협이 많았던 네트워크 CCTV의 보안 취약성을 중심으로 공격 상황에서 관제 성능의 저하 정도를 분석 해 보았다.

4.1 CCTV 관제 성능 분석 대상

본 절에서는 부산시 교통정보서비스 센터에서 운용중인 VICIOS를 GIS상에 표출한 가상 지도를 기반으로 하여, 관제시스템에 대한 악의적인 회피 상황을 제시하였다. 그리고 그 결과를 토대로, 관제 성능의 저하 정도를 일반화하기 위해 수식을 작성하였다.

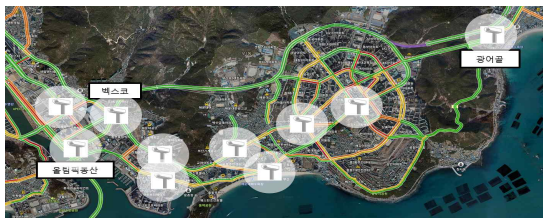


그림 2. 부산시교통정보센터에서 제공하는 관제 CCTV(‘다음 지도’ 활용)

4.2 CCTV 회피로 인한 관제 성능 저하 분석

그림 3은 송정동의 ‘광어골’(우측상단)에서 민락동 ‘올림픽 동산’(좌측하단) 방향으로 도주하는 경우에, 도주차량이 포착될 수 있는 CCTV와 예상 경로를 요약한 것이다. 간략화를 위해서 교통관제 CCTV가

부착된 큰 도로만 나타내었고, 우측상단의 '광어골' 의 CCTV의 첫 번째 기로에서부터 최종 '올림픽 동산' 진입로 방향으로 총 11개의 기로가 있다.

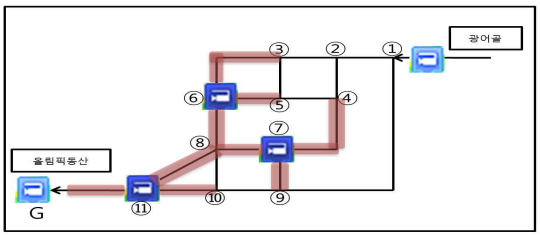


그림 3. VICIOS CCTV 탐지 경로

이 간소화된 도로 감시 상황을 토대로, 해킹상황, 즉 악의적으로 CCTV의 방향을 제어하여 예측한 도주로의 화면을 촬영 할 수 없게 하거나, 물리적으로 동작을 멈추게 했을 상황을 고려할 수 있다.

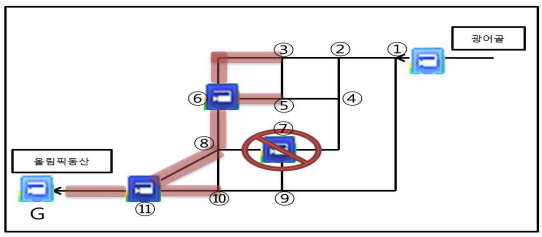


그림 4. 한 대(⑦)의 카메라가 관제 불능 상태일 때

그림 4는 ⑦-CCTV가 모니터링 불능 상태로, 도로의 차량을 감지할 수 없을 때를 나타낸 그림이다. 그림 3과 비교하여 붉은색 관제 영역이 감소 한 것을 볼 수 있다.

4.3 CCTV 관제 성능 저하 일반화 수식

본 절에서는 정상 운용될 때와 CCTV가 동작 불능 상태가 되었을 때의 관제 성능을 비교하기 위해 일반화된 수식을 작성하였다. 단, CCTV가 정상적으로 운용될 때에는 '광어골', '올림픽동산' CCTV를 제외한 해운대 시내의 3대의 교통 감시 카메라를 적용했다.

먼저 관제 기로(Node : N)를 대상으로 한 수식으로 관제율을 계산 할 수 있다. 감시 카메라는 전체 11개의 기로 중에서, ③, ⑤, ⑥, ⑧, ⑩, ⑪ 총 6개의 기로를 관제하게 된다. 반면, ⑦-CCTV가 관제 불능 상태일 때는 기존 6개의 관측 가능한 기로 중에서 ④, ⑨가 관측 불가능 하게 된다. 즉, 정상적인 운용 중에는 기로위에 설치된 각각의 카메라의 대수에 비례해서 삼거리, 혹은 사거리의 교차수를 고려하면, 전체 감시중인 기로의 개수를 알 수 있다. 또한, 일직선 도로상의 감시카메라 C_0가 제거된 C_n의 수를 파악해야 한다. 수식으로 정리하면 다음과 같다.

$$N_{on} = (\sum C_l - \sum CI_m - \sum CA_n) \times w \times 2 \quad (1)$$

where,

N_{on}(Node-on) : 감시중인 기로

w : 도로의 교차 수, 삼거리, 사거리 등

C_l(Camera) : 기로상의 감시카메라

CI_m(Camera-Ignored) : 일직선 도로상의 카메라

CA_n(Camera-Adjoined) : 카메라들이 인접해있는 관계의 수

전체 기로 중에서 관제 가능한 기로의 비율을 계산한 관제율 S_N은 다음과 같다.

$$S_N = \frac{N_{on}}{N_{tot}} \times (100\%) \ ,$$

$$\text{단, } N_{tot} = (N - \sum CA_n) \times w \times \frac{1}{2} \quad (2)$$

where,

S_N(Surveillance from Node) : 기로에 의한 관제율

N(Node) : 실제 기로의 개수

N_{tot}(Node-total) : 이상적인 전체 기로의 개수

N_{on}(Node-on) : 감시 가능한 기로

한편, 기로와 기로 사이는 도로(Link : L)로 정의한다. 정상 운용 상태일 때는 전체 17개로 구분된 도로 중에서 9개의 도로를 관제하는 것으로 볼 수 있다. ⑦-CCTV가 사용 될 수 없을 경우, 3개가 줄어든 6개의 도로로 관제 가능한 도로수가 줄어든다. 이와 같은 결과를 기반으로 관제 가능한 도로에 관한 수식을 도출해낼 수 있다.

$$L_{on} = (\sum C_n - \sum CI_m - \sum CA_n) \times w \quad (3)$$

where,

L_{on}(Link-on) : 감시중인 도로

기로 위의 유효한 카메라와 그 기로의 도로 개수를 곱하면, CCTV가 관제하는 도로의 전체수를 구할 수 있는데, 단 중복되는 도로를 제거해야 한다. 이에 관한 관제율을 구하기 위한 수식은 다음과 같다.

$$S_L = \frac{L_{on}}{L_{tot}} \times (100\%) \ ,$$

$$\text{단, } L_{tot} = (L - \sum CA_n) \times w \qquad (4)$$

where,

S_L(Surveillance from Link) : 도로에 의한 관제율

L(Link) : 실제 도로의 개수

L_{tot}(Link-total) : 이상적인 전체 도로의 개수

L_{on}(Link-on) : 감시 가능한 도로

삼거리에 놓인 감시카메라는 기로 전방의 두 개의 도로가 판단 가능하다. 양 쪽 도로의 차량 모두를 카메라에 포착하는 것이 이상적이지만, 카메라가 두 도로 중 하나만 촬영하더라도, 반대방향으로 통과한 것을 예측할 수 있기 때문이다. 그리고 전방의 관제 대상은 반드시 카메라의 후방으로 통과하기 때문에 결국 카메라의 세 방향이 관제가 가능하다.

그림 3,4와 같이, 3대의 기로상의 감시카메라가 모두 동작할 때부터 하나씩 동작 불능 상태가 될 때, 기로·도로의 관제율 수식을 계산한 결과는 다음과 같다.

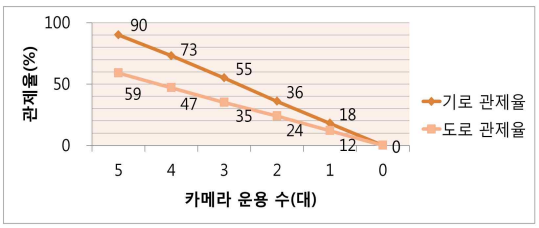


그림 5. 도로의 감시상태와 관제율의 저하

Ⅴ. 결 론

민간 및 공공기관의 CCTV의 설치 대수는 앞으로도 계속 증가할 것이며, 따라서 영상관제의 범위가 넓어질 뿐만 아니라, CCTV 카메라의 위치를 전자지도에서 파악하고 정보를 활용할 수 있는 기회가 늘어날 것이다[12]. 그러나 통신 네트워크의 규모가 커질수록 보안 위험성은 커지게 되어, 위치정보 등의 데이터의 노출이 심해질 것이다. 또한 하위 단말기의 접점이 많아지는데, 이는 중앙 컨트롤 센터로의 접근 방법이 많아지는 것을 의미한다.

따라서 본 연구에서는 현재 네트워크 CCTV의 해킹 방법들은 연구하고, 현재 운용중인 CCTV로의 침투 시나리오를 작성하고, 접근 실험을 실시했다. 대부분의 네트워크 CCTV가 IP기반의 웹브라우저 컨트롤로 제공된다는 점을 감안해서, 영상처리 서버 혹은 직접 CCTV의 영상 서버의 IP를 탐색해내고, 일반적인 네트워크 해킹의 방법으로 접근할 수 있는 가능성을 염두에 두어 두고 있으며, 관리자의 보안 관리의 취약점을 이용한 무단 접근 방법을 고려 해 볼 수 있다.

3장에서 제시한 CCTV 관제 성능 저하 분석과 더불어 CCTV 카메라의 실제 촬영 방향, 소 도로와의 교차점, 비공개된 교통 및 방범용 CCTV위치 및 설치 대수를 고려한 정밀한 분석은 GIS 네트워크 분석, 버퍼링 분석 등으로 추후 연구에서 실시하여, CCTV의 보안 강화와 효율적인 설치 장소를 분석하는데 활용 할 수 있을 것이다.

참 고 문 헌

[1] Taewoong Seo, Myunggyun Jeong, and Changsoo Kim, “A Study on Vulnerabilities of Monitoring and Control System based on IT Convergence Technology,” *The 6th International Conference on Multimedia Information Technology and Applications*, pp. 245-247, 2010.

[2] 유지영, 이재일, “신규 IT 서비스 도입 확산을 위한 정보보호,” 한국정보처리학회 정보처리학회지, 제17권, 제2호, pp. 10-17, 2010.

[3] 서태웅, 김창수, 이재승, 이철원, “지리정보시스템과 관제시스템의 융합에 관한 연구,” 한국멀티미디어학회논문지, 제14권, 제5호, pp. 703-709, 2011.

[4] 김영진, 이수연, 권헌영, 임종인, “국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구,” 한국정보보호학회논문지, 제19권, 제1호, pp. 103-111, 2009.

[5] R. Bejtlich, *Tao of Network Security Moni-*

toring, the beyond Intrusion Detection: What is Network Security Monitoring, Addison Wesley Professional, 2004.

[6] 오영균, "CCTV통합운용을 위한 제도개선에 관한연구," 한국행정학회 2009년도 공동학술대회 발표논문집, pp. 302-319, 2009.

[7] 강원지방경찰청 홈페이지 "http://www.kwpolice.go.kr"

[8] 이원규, 주수현, "CCTV 통합구축 민간투자사업(BTL) 타당성 및 관제센터 구축방안 연구," 부산발전연구원, 2011.

[9] 이문구, "정보시스템 보안관리를 위한 위험분석 방법론," 전자공학회논문지, 제41권, 제6호, pp. 13-22, 2004.

[10] Johnny Long, 구글해킹 절대내공, 에이콘출판주식회사, 2010.

[11] 윤은준, "CCTV 시스템에서의 보안 위협 요소," CCTV NEWS, 연재 7, 2010.

[12] 권원석, 이현곤, 김영섭, 김창수, "GIS를 활용한 지능형 교통제어 시스템과 재난 정보의 연계," 2010 한국지리정보학회 춘계 학술발표대회 논문집, pp. 130-131, 2010.

서 태 웅

2010년 부경대학교 컴퓨터멀티미디어공학과 학사
2010년~현재 부경대학교 IT융합응용공학과 석사과정
관심분야 : 소셜네트워크서비스, 보안관제, 재난정보관리, 지리정보시스템

이 성 렬

2001년 서강대학교 컴퓨터학과 학사
2003년 서강대학교 컴퓨터학과 석사
2010년 서울대학교 컴퓨터공학과 박사
2010년~현재 ETRI 부설연구소

배 병 철

1994년 홍익대학교 컴퓨터공학과 학사
1996년 홍익대학교 전자계산학과 석사
2005년~현재 충남대학교 컴퓨터공학과 박사과정
1996년~1999년 국방정보체계연구소 연구원
1999년~2000년 국방과학연구소 연구원
2000년~현재 ETRI 부설연구소 과제책임

윤 이 중

1988년 인하대학교 전자계산학과 학사
1990년 인하대학교 전자계산학과 석사
2002년 충남대학교 컴퓨터공학 박사
1991년~2000년 ETRI 정보보호연구단
2000년~현재 ETRI 부설연구소 선임본부장

김 창 수

1991년 중앙대학교 컴퓨터공학과 박사
2006년~현재 유비쿼터스 부산 도시협회 방재분과위원장
2006년~현재 (사)그레고리장학회 이사

2011년~현재 한국멀티미디어학회 정책자문위원
1992년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 방재IT, UIS/GIS, 운영체제, 시멘틱 웹, 재난관리, 공간검색, 도시방재 등