Journal of Korea Multimedia Society Vol. 18, No. 5, May 2015(pp. 631-640)
http://dx.doi.org/10.9717/kmms.2015.18.5.631

TCP 세션을 활용한 사설망 구간 CCTV 단말의 생사판별 알고리즘

신해준†, 정연기††

Device Alive Check Algorithm using TCP Session under CCTV Network based on NAT

HaeJoon Shin†, YounKy Chung††

ABSTRACT

Recently CCTV system is installed widely purpose to enhanced physical security, gathering criminal evidence and management of facilities. In spite of supporting strong management function, CCTV system has weak security function. Therefore high security management function is required. Generally it's not easy to control the devices under NAT using a NMS(Network Management System). So we design and implement alive check algorithm of CCTV devices under NAT using DVRNS address resolution and TCP session check. We evaluated and analyzed of developed system on real environment which includes about 100 DVRs under NAT. As a result of test, it showed that device alive check and DVRNS address resolution were well performed without any error.

Key words: DVRNS, NAT, Alive Check, Port Forwarding, Fault Management

1. 서 론

최근 물리적 보안 강화와 범죄 증거 확보를 위한 목적으로 CCTV(closed circuit television) 가 많이 활용되고 있으며 국내에서는 2009년 기준, 약 274만대(공공 설치 24만대, 민간 설치 250만대)였던 CCTV가 2013년 말 현재 약 400만대(공공 설치 56만대, 민간 350만대 추산) 이상 설치된 것으로 추산된다[1,2]. 공공용 CCTV는 용도별로 어린이 안전, 재난·화재 감시목적의 생활안전용과 교통단속, 쓰레기 투기 방지 등의 법규위반 단속용, 그리고 지하철, 철도, 우체국, 주차관리, 시설물 보호 등의 시설물 관리용으로 사용되고 있다. 그러나 현재의 CCTV 장치 등은 보안이 매우 취약한 상태에서 관리되고 있기 때문에 악의적인 공격으로 CCTV의 순기능이 운영되지 않을 수 가능성이 높아 이를 위해서는 반드시 영상 및 저장장치에 대한 보안 관리 기술들이 연구되어야 한다.

초기에 구축된 대부분의 CCTV 시스템은 영상장치로는 아날로그 카메라, 저장장치로는 DVR(Digital Video Recorder)를 활용하고 네트워크는 ADSL 기반의 사설망으로 구축되었고, CMS(Central Monitoring System)을 통해서 영상을 관제하고 장애의 판단은 관리 요원의 육안판단에 의존하고 있다. 현재는 디지털 카메라, NVR(Network Video Recorder) 및 전용망으로 구축되고 있는 추세이며 관리를 위해 VMS(Video Management System)과 IP 관리제품

※ Corresponding Author: YounKy Chung, Address: (712-701) 50, Gamasil-gil, Hayang-eup, Gyeongsan-si, Gyeongbuk, Korea, TEL: +82-53-600-5565, FAX: +82-53-600-5579, E-mail: ykchung@kiu.ac.kr
Receipt date: Sep. 18, 2014, Revision date: Oct. 8, 2014
Approval date: Nov. 3, 2014

† Research Center, NetMan Co., Ltd.
(E-mail: fisher@netman.co.kr)
†† Dept. of Computer Eng., College of IT Convergence, Kyungil University
※ This study was supported by the Kyungil University Grant.

을 활용하고 있다. 전용망 기반의 CCTV의 관리는 일반적인 네트워크 장비의 관리기능으로 관리가 가능하나 ADSL을 사용하는 NAT 기반의 CCTV의 경우 공유기 하부에 연결되어 있어 일반적인 네트워크 관리기능으로는 관리가 불가능하다. 현재 전국에 설치된 CCTV중 약 65% 정도가 NAT 기반인 것으로 추정되고 있어 이를 위한 관리방안의 연구가 필요하다. 지금까지 NAT 하위 단말의 통신 및 관리 문제를 해결하기 위해 P-CSCF (Proxy-Call Session Control Function)를 활용한 NAT Traversal 문제 해결 방안[3], NAT 환경에서 UDP Hole Punching 방법을 SNMP 프로토콜 상에서 적용하는 방안[4] 및 인터넷 공유기 내부의 사설 IP주소가 설정된 인터넷 전화단말을 효율적으로 관리하고 제어하기 위한 인터넷 전화단말 원격관리시스템 개발 등의 연구가 진행되었다[5-7].

본 논문에서는 TCP 기반의 응용에 적용이 가능하고 또 SNMP 등과 같이 별도의 관리 프로토콜을 사용하지 않는 사설망 기반의 CCTV 단말의 생사판별 알고리즘을 개발 하고자 한다. 본 논문의 2장에서는 아날로그 CCTV와 디지털 CCTV의 구성을 살펴보고, 3장에서는 제안 알고리즘의 세부구성 및 동작 원리를 살펴보고, 4장에서는 실험결과를 정리하고 5장에서 본 논문의 결론을 맺고자 한다.

2. 관련연구

2.1 Analog CCTV의 구성

현재 공공기관에서 많이 사용되고 있는 CCTV는 아날로그 카메라와 DVR로 구성된 아날로그 CCTV와 디지털 카메라, NVR로 구성된 디지털 CCTV로 크게 구분될 수 있다. 아날로그 CCTV에서 사용되는 저장장치인 DVR은 1990년대 후반 도입된 저장장치로 감시카메라로 입력된 영상 데이터를 디지털 신호로 전환하여 하드디스크 등에 압축・저장하는 영상보안장치이다. 아날로그 CCTV에서는 DVR이 아날로그 카메라에서 동축케이블을 통해 전송 받은 신호를 디지털 신호로 변환하여 저장한다. Fig. 1과 Table

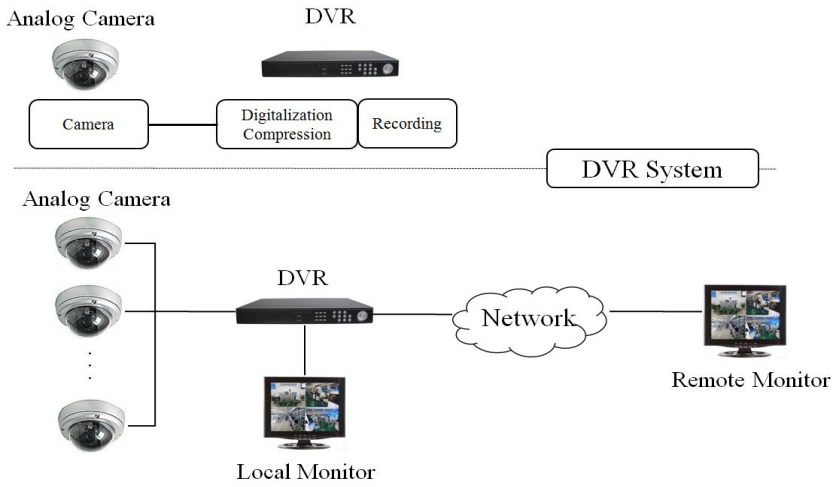

Fig. 1 Structure of Analog CCTV system.

Table 1. Analog CCTV Elements

Elements	Remarks	Managed Object
Analog Camera	Number of Camera depends on DVR's performance	No
DVR	Require variable cables for connecting to camera (BNC cable, UTP cable etc.)	Yes
Monitoring device	Must be into CCTV facility Require extra fund to remote control and integration operation	-

1은 아날로그 CCTV의 구성도 및 특성을 나타내고 있다.

일반적으로 아날로그 CCTV는 ADSL에 연결되어 공유기(NAT) 하부에 설치되어 운영되고 있으며, 전국에 설치된 CCTV의 약 65%를 차지하고 있다[8]. 아날로그 CCTV에서의 관리대상 장비는 IP를 가진 DVR이며 카메라는 DVR과 동축케이블로 연결되어 있으므로 관리대상에 포함되지 않는다. 또한 DVR은 대부분이 공유기에 연결되어 있기 때문에 1) 외부망에서 직접 연결할 수 없고, 2) ADSL에 연결된 공유기가 DHCP에 의해 IP를 할당받으므로 IP주소가 주기적으로 변경되어 일반적인 망관리 기술로는 제어가 불가능하다. 현재 대부분의 아날로그 CCTV는 CMS(Central Monitoring System)을 기반으로 CCTV가 송출하는 개별 모니터 영상을 확인을 통해 장애 유무를 확인하고 있어 효율성이 매우 떨어진다. 그러므로 본 논문에서는 NAT 하부의 CCTV 장비에 대한 효율적인 생사판별 기술을 제안하고자 한다.

2.2 Digital CCTV의 구성

디지털 CCTV는 아날로그 카메라에서 제공되는 아날로그 스트림을 녹화하는 DVR과 달리, 디지털 카메라에서 이미 인코딩된 디지털 비디오 스트림을 NVR에 녹화한다. 또한 동축케이블을 사용하는 DVR와 달리 네트워크 케이블을 이용하여 설치가 용이하고 카메라의 위치와 개수에 구애받지 않고 설치가 가능하다. Fig. 2와 Table 2에서는 디지털 CCTV의 구성과 특성을 나타내고 있다.

현재 신규로 구축되는 대부분의 CCTV 통합관제센터는 디지털 CCTV 형태로 구축된다. 네트워크 관리 관점에서는 디지털 카메라와 NVR 등이 관리대상 장비에 포함될 수 있다. 디지털 CCTV 장비의 경우 대부분이 IP를 가진 네트워크 장비로 분류될 수 있기 때문에 일반적인 망관리 기술로 관리가 가능하다. 현

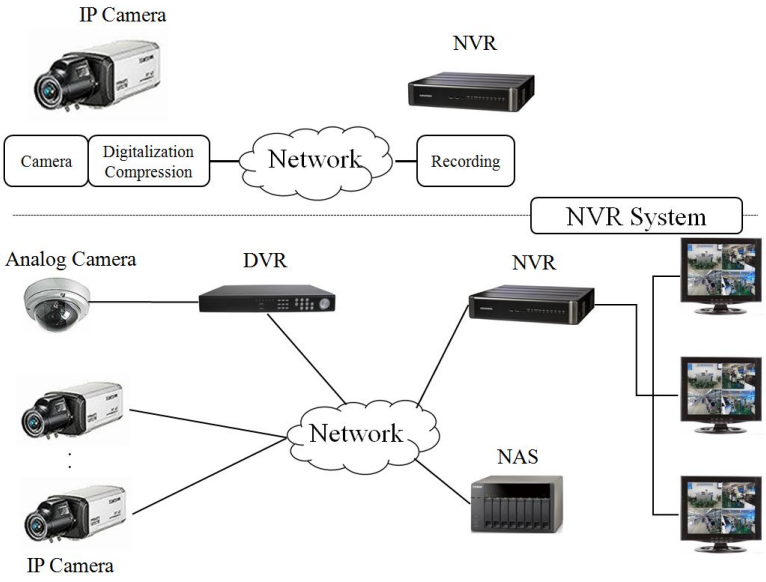

Fig. 2 Structure of Digital CCTV system.

Table 2. Digital CCTV Elements

Elements	Remarks	Managed Object
IP Camera (Digital Camera)	Number of IP camera in unlimited	Yes
Network	Use legacy LAN environment	-
NVR	Possible to manage large data	Yes
Monitoring device	Not depend on physical position several person can monitor simultaneously	-

재까지 구축된 CCTV 관제센터에서는 디지털 CCTV의 관리를 위해 VMS(Video Management System)와 IP관리솔루션(또는 NMS)이 함께 사용되고 있어 장비의 생사판별과 관리기능은 충분히 제공되고 있다. 그러므로 본 논문에서는 디지털 CCTV에 대한 관리기능 연구는 포함하고 있지 않으며 디지털 CCTV의 경우 보안의 관점에서 보완해야 할 많은 연구 분야가 필요할 것으로 판단된다[9].

3. TCP 세션을 활용한 사설망 구간 CCTV 단말의 생사판별 알고리즘

3.1 제안 알고리즘의 개요

본 논문에서는 사설망 구간에 존재하는 CCTV 장비의 생사판별 알고리즘을 제안한다. Fig. 3은 NAT 기반의 CCTV의 생사판별 알고리즘의 전체적인 흐름도를 나타내고 있다.

NAT 기반의 CCTV 시스템은 아날로그 카메라, DVR, 공유기, DVRNS(DVR Name Service) 등으로 구성되어 있으며 관리적인 특성은 아래와 같다.

1) 대부분의 DVR은 도메인 네임(Domain Name)으로 관리된다. DVR은 공유기(NAT) 하부에 연결되어 있고, 또한 DVR이 연결된 공유기의 IP가 주기적으로 변경되므로 일관성 있는 접근이 가능하도록 IP 주소 대신 도메인 네임을 사용한다.

2) DVR이 연결된 공유기의 공용 IP 획득을 위해서 DVRNS를 사용한다. 일반적으로 공유기의 IP를 획득하는 방법은 DVR에 도메인 네임을 할당하여 관리하는 경우 DVRNS를 사용하고, 공유기에 도메인 네임을 할당하는 경우 DDNS(Dynamic DNS)를 사용한다. 본 논문에서는 실제 현장에서 가장 많이 활용하고 있는 DVRNS를 기본으로 하여 실험하였다.

3) DVRNS는 표준 프로토콜이 아니며, CCTV 제조사들의 특정 어플리케이션을 통해서만 사용이 가능하다. 본 논문에서는 역공학을 통한 DVRNS 프로토콜을 분석하여 테스트 어플리케이션에서 적용할 수 있도록 재설계 하였다.

3.2 DVRNS 변환

앞서 언급한 대로 공유기 하부의 DVR은 도메인 네임을 부여하여 관리한다. 하지만 실제 관리 시에는 DVR이 연결된 공유기의 IP를 획득해야 한다. 이때 DVR의 도메인 네임을 공유기의 IP로 변환해 주는 것이 DVRNS 서버의 역할이다. 본 논문에서는 DVR의 도메인 네임를 활용하여 공유기 IP를 획득할 수 있도록 Fig. 4와 같이 DVRNS의 기능을 이용하여 구현하였다.

DVRNS를 통해 DVR이 연결된 공유기의 IP를 획득

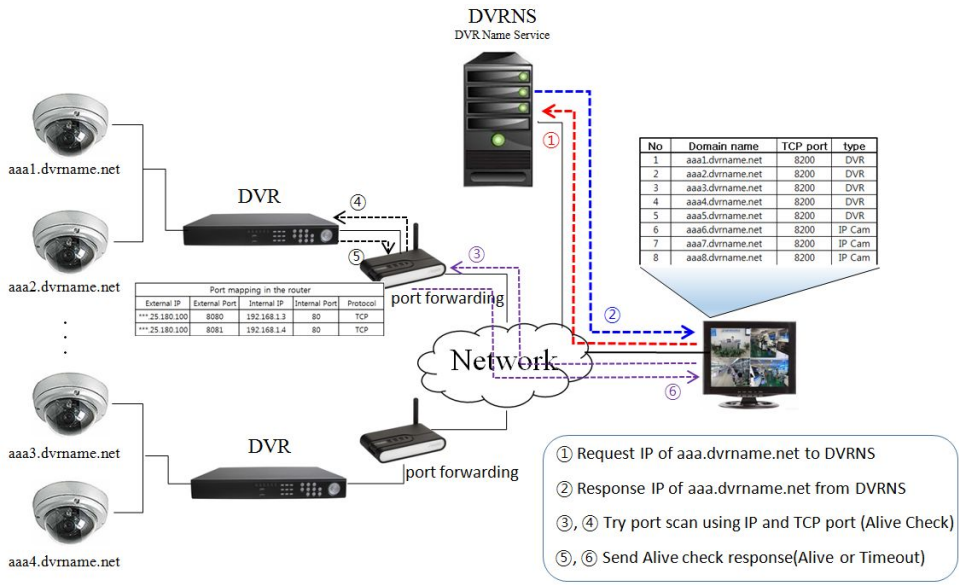

Fig. 3. Alive Check algorithm for CCTV device under NAT.

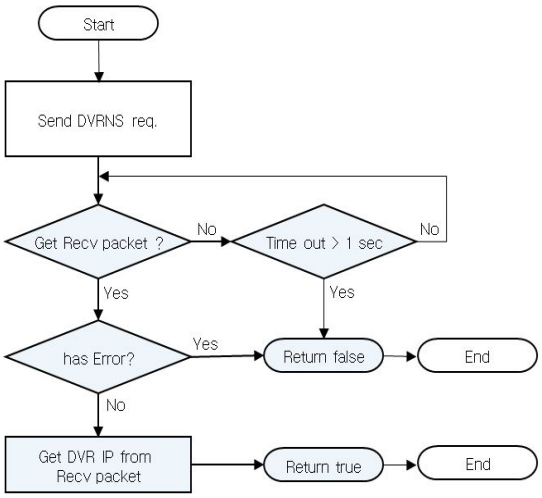

Fig. 4 Flow chart of Naming Resolution using DVRNS.

하기 위한 통신 프로토콜의 수행절차는 다음과 같다.

1. 관리자는 DVRNS 서버에 접속한다. 이때 서버에 접속하기 위한 기본 정보인 DVRNS 서버의 주소, 서비스 포트번호가 필요하다.
2. 도메인 네임에 대한 IP를 획득하기 위한 질의 요청 패킷을 전송한다.
3. 응답패킷을 수신하여 IP를 획득한다.

3.2.1 요청 패킷

Fig. 5는 역공학을 통해 분석한 DVRNS 패킷의 TCP/IP 헤더를 제외한 데이터부분의 구조이다. Domain name과 Local IP 필드에는 문자열을 입력하며, Domain name 필드에는 DVR의 도메인 네임을 입력하고 Local IP는 요청 서버의 공용 IP를 입력하여 요청한다. DVRNS 요청패킷의 기타 필드에 대한 설명은 본 논문에서는 배제하였다.

3.2.2 응답 패킷

DVRNS 요청패킷에 대한 응답패킷의 구조는 Fig. 6과 같으며 해당 DVR의 도메인 네임이 Domain Name 필드에 포함되어 있고, Target IP 필드가 공유기의 공용 IP를 포함하고 있다. DVRNS 응답패킷의 기타 필드에 대한 설명은 본 논문에서는 배제하였다.

3.3 Port Forwarding

사설 IP 주소를 가지는 네트워크 장비들은 인터넷에 접속하기 위해 NAT 기능을 이용한다. NAT (Network Address Translation)는 사설 IP 주소를 공용 IP 주소로 변환하는 기능과 인터넷에서 사설망에 속한 네트워크 자원에 접속할 때 NAT의 공용 IP 주소로 들어온 요청을 사설망 내의 목적지 자원에 전달하는 기능을 수행한다.

사설망 내에 하나 혹은 여러 개의 장비가 애플리케이션 서비스를 제공하는 경우 지정된 목적지에 데이터를 전송하기 위해 NAT는 포트 포워딩 기능을

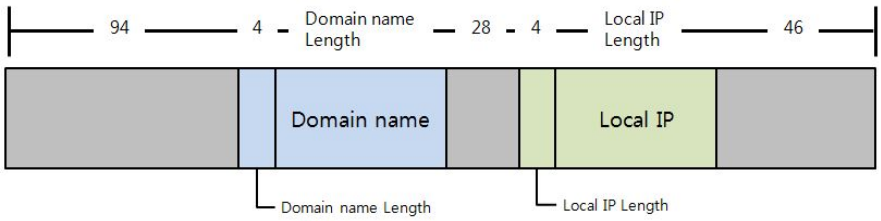

Fig. 5 Structure of DVRNS Request Packet.

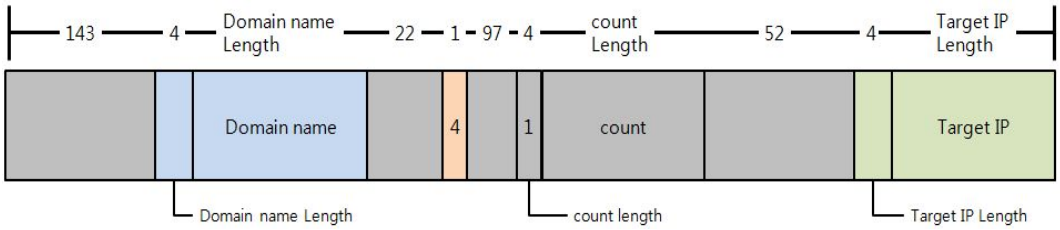

Fig. 6 Structure of DVRNS Response Packet.

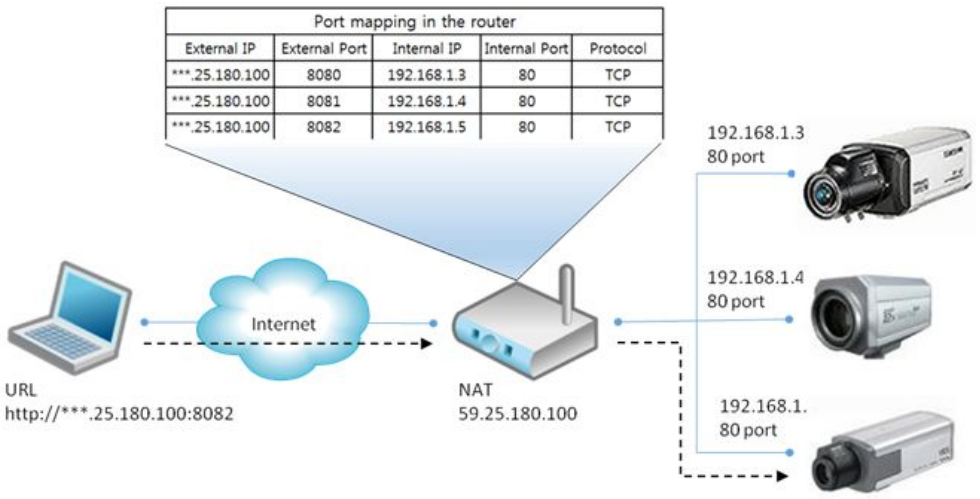

Fig. 7 Port Forwarding procedure.

이용한다. Fig. 7과 같이 사설망 내부에 80번 포트를 이용하는 하나 이상의 디지털 카메라가 존재하는 경우, NAT는 특정 장비의 HTTP 포트를 내부망에 유일한 포트 번호로 매칭하여 미리 정의된 포트 테이블을 구성한다. 인터넷에서 NAT로 들어오는 패킷은 NAT의 공용 IP 및 유일한 서비스 포트 정보로 패킷을 전달하고, 해당 패킷을 수신한 NAT는 해당 포트 정보와 매칭된 장비 및 매칭된 포트 번호로 목적지 주소정보를 변환하여 패킷을 전달한다. 이때 변경된 패킷의 송신자 정보는 NAT의 사설 IP 주소로 변경된다. 외부로 전달되는 패킷 또한 동일한 원리로 동작한다.

3.4 Alive Check

사설 IP 주소를 가지는 네트워크 장비들의 생사를 판별하기 위해서 일반적인 전용망에서 장비의 생사를 판별하기 위한 ping 기능을 이용할 수 없다. NAT 하부의 장비들이 외부 네트워크에서는 숨겨진 네트워크이기 때문에 외부에서 접속하기 위한 공용 IP는 공유기를 사용하는 경우 공유기에 설정된 IP가 유일하다. 하지만 망관리 관점에서는 관리대상 장비의 생사 판별은 매우 중요한 영역이므로 이를 위한 다양한 방법을 사용할 수 있다.

첫째, 사설망 내부에 에이전트를 설치하여 에이전트가 생사를 판별하고 생사 정보를 관리시스템에게로 전송하여 해당 시스템을 관리한다. 둘째, 사설망 내부의 에이전트 설치는 추가 비용을 발생시키므로 이를 해결하기 위해서는 공유기의 포트 포워딩 기능을 활용한 연결성 체크 방법을 활용할 수 있다. 이는 TCP의 3-way handshake를 응용한 방법이며, 본 논문에서는 이을 이용하여 NAT 하부의 장비에 대한 생사 판별을 수행한다.

Alive Check 서비스는 지정된 호스트 주소와 TCP포트 번호를 사용하여 TCP연결 유무를 판별하는 서비스로, 그 구성은 Fig. 8과 같고 Fig. 9에서 Pseudo code를 보여주고 있다.

4. 실험 결과 및 고찰

본 연구에서는 NAT 기반 CCTV를 대상으로 Alive Check 기능을 수행할 수 있도록 구현하였다. 약 100대의 DVR 장비로 구성된 실제 운영 중인 ADSL 기반의 CCTV 망에 적용하여 실험하였고, 공유기에는 DVR이 사용하는 Port에 대한 Port Forwarding을 설정하였다. Fig. 10은 구현 결과를 보여주고 있는데, 각각의 아이콘이 DVR 장비를 의미하고 동작하지 않는 장비에 대해서는 X 표시로 구분하도록 하였다. 화면의 우측에는 선택된 장비의 정보와 종류, 그리고 도메인 네임 등이 표시되도록 하였다. 본 연구에서 수행한 생사판별 결과를 실제 CCTV 화면과 비교해 본 결과 실험 환경에서 정상적으로 기능 동작하는 것을 확인하였다.

Fig. 11은 각 CCTV 단말들의 관리포트를 등록하

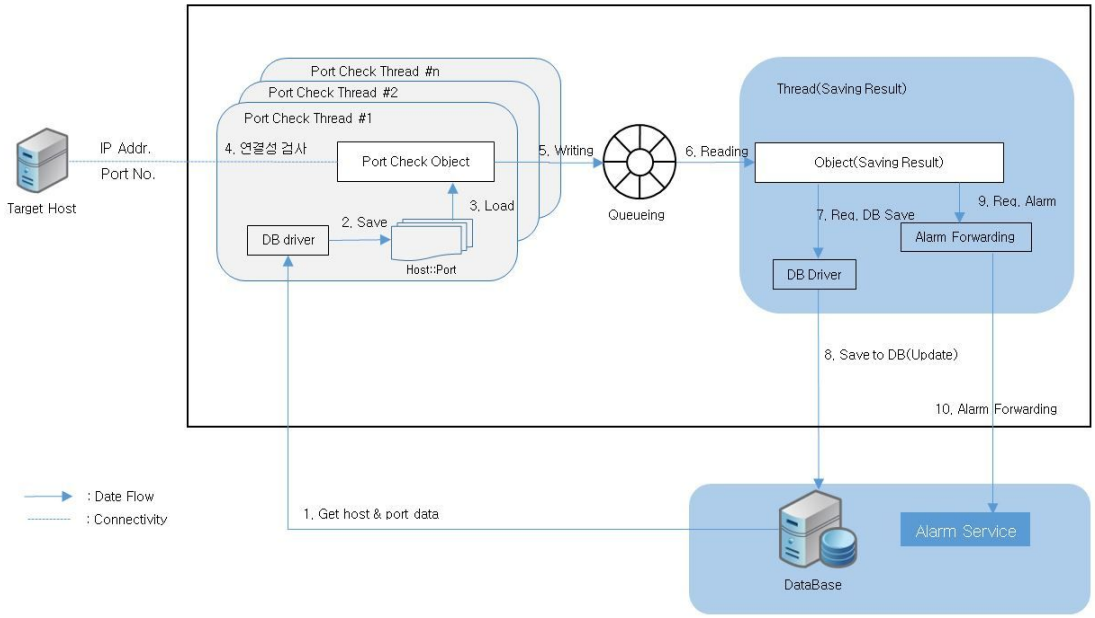

Fig. 8. Alive Check procedure.

```
//Getting IP Address from DVRNS Hostname
INT CDVRNSQThread::GetIpAddressFromHostName()
{
  ...
 for(INT idx = 0; idx < nCnt; idx++)
  {
   // get host info
  }

  m_dvrnsinfo.GetDVRNHostNameFromDB();
  GetIpAddressFromDnsHostName();
  m_dvrdomainlist.GetDVRNSListFromDB();

  //Get IP address
  for(pos = begin; pos != end ; ++pos)
  {
    //if it use DVRNS domain address
    if(pos->strHostName == TRUE)
    {
      //Get IP from DVRNS
    }
    else
    {
      //Get IP form DNS
    }
  }

  return 0;
```

```
//Alive Check
int PCheck::port_scan(struct sockaddr_in* dest)
{
   ...
 // set time out = 1sec
  timeouts.tv_sec = 1 ;
  timeouts.tv_usec = 0 ;

  // create socket
  fd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
   ...
   // Non blocking status
  fcntl(fd, F_SETFL, newSockStat)

  // Try to connect
  connect(...);

  if ( (n = select(...)) == 0)
  {
    // timeout
    ...
    return FALSE;
  }
   …
   return TRUE;
}
```

Fig. 9. Pseudo-code of Alive Check.

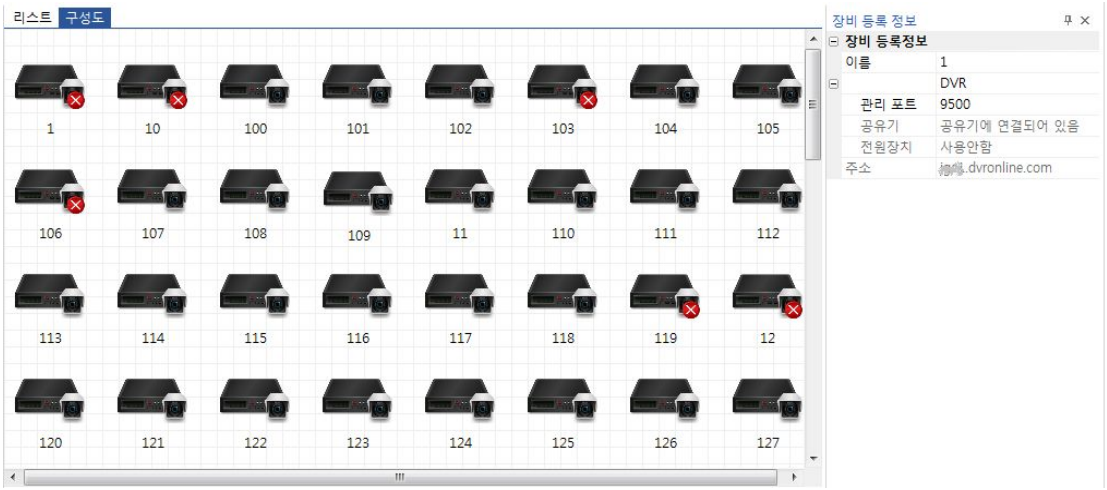

Fig. 10. Console view of CCTV Alive Check.

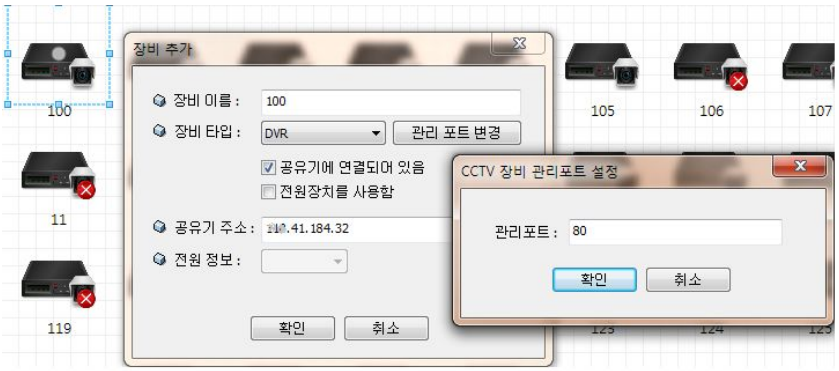

Fig. 11. Setting for Port Check.

는 화면을 보여주고 있다. 단말의 제조사에 따라서 사용하는 포트가 상이하므로 관리시스템에서는 개별/전체 단말의 관리포트를 등록하도록 하였다. 본 연구에서 제안하는 NAT망 뿐만 아니라 공용망에서도 적용이 가능하도록 설계하였다.

Fig. 12는 DVRNS의 동작 결과를 보여주고 있다. DVR 각각의 도메인 네임에 대한 IP주소가 정상적으로 획득하는 것을 확인할 수 있었다. 또한 공유기에 도메인 네임을 적용한 DDNS를 이용한 IP 획득도 가능하였고 이를 이용한 DVR의 생사판별도 동일한

Fig. 12 result of DVRNS Name Resolution.

Table 3. Test Result

Function	Result	Target Device		
		NAT Device	DVR	Digital Camera
DVRNS Resolution	○	(DDNS)	○	○
Alive Check	○	-	○	○
Port Forwarding	○	○	-	-

결과를 나타내었다.

5. 결 론

본 논문에서 제안한 TCP 세션을 활용한 사설망 구간 CCTV 단말의 생사판별 알고리즘을 실제 운영중인 CCTV 환경에서 실험하였고 기능적 완성도를 높이기 위해 관리대상 CCTV 단말에 임의적인 장애의 상황을 만들어 추가하였으며 실험결과 단말의 생사판별이 정확하게 수행되었다. 이를 통해 NAT 구간의 CCTV 단말에 대한 정확한 생사 확인이 가능하였고, 도메인 네임으로 관리되는 단말의 IP주소변환 기능도 정상적으로 동작하는 것을 확인할 수 있었다. Table 3은 본 논문의 최종적인 실험 결과를 보여주고 있다.

본 연구를 통해 NAT 기반의 CCTV 단말의 관리 기능을 설계하고 구현한 결과물을 실제 CCTV 환경에서 테스트하였다는 점에서 큰 성과가 있었으며, 향후 사설망 CCTV와 전용망 CCTV가 통합되어 운영되는 통합관제센터에 적용이 가능할 것으로 판단된다. 향후 연구에서는 관제센터에서 추가적으로 요구되는 관리기능의 추가와 현장에 바로 적용이 가능하도록 기능을 확장하고자 한다.

REFERENCE

[1] National Human Rights Commission, *CCTV Installation and Operation of Private Sector*, 2010.

[2] CCTV installation rate of Government office(e-national index), http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=2855 (accessed Sept., 2, 2014).

[3] S.J. Han, J.O. Lee, and S.C. Kang, "The Efficient Scenario of Solving NAT Traversal in the IMS," *Journal of the Korea Academia-Industrial Cooperation Society*, Vol. 14, No. 4, pp. 1935-1941, 2013.

[4] C.G. Park, S.G. Kim, K.T. Jeung, and Y.S. Lee, "A Remote SNMP Connection Request Mechanism for NATed Devices using UDP Hole Punching and Heuristic Hole Binding Time Search," *Journal of the Korea Institute of Information Scientists and Engineers*, Vol. 35, No. 4, pp. 367-373, 2008.

[5] H.C. Song and K.I. Ban, "Development of Remote Management and Control System for VoIP Terminal," *Journal of the Institute of Internet, Broadcasting and Communication,* Vol. 11, No. 6, pp. 73-80, 2011.

[6] J.C. Han and S.G. Kang, "NAT Traversal of SIP User Agent," *Proceeding of the Korean Institute of Maritime Information and Communication Sciences,* Vol. 9, No. 2, pp. 579-581, 2005.

[7] S.M. Lee and K.B. Lee, "Design and Implementation of Multipoint VoIP, using End-point Mixing Model," *Journal of Korea Multimedia Society*, Vol. 10, No. 3, pp. 335-347, 2007.

[8] CCTV Security leads 'Safety Korea', http://www.etnews.com/201304290205 (accessed Sept., 11, 2014).

[9] CCTV, Advance guard of Safety Korea. http://www.etnews.com/20140403000037 (accessed Sept., 11, 2014).

신 해 준

1999년 2월 영남대학교 대학원 정보통신공학과(공학석사)
2003년 2월 영남대학교 대학원 정보통신공학과(공학박사)
2004년 8월~2012년 2월 영진전문대학 컴퓨터정보계열 교수
2012년 3월~현재 (주)넷맨 연구소 기술책임자
관심분야: 정보보안, 네트워크보안, 융합보안

정 연 기

1990년 3월~현재 경일대학교 자동차IT융합대학 컴퓨터공학과 교수
1998년 1월~1998년 12월 호주 뉴캐슬대학교 컴퓨터공학과 방문교수
2008년 1월~2008년 12월 한국정보과학회 부회장
2009년 1월~2009년 12월 한국멀티미디어학회 부회장
관심분야: 멀티미디어 통신, 통신망 관리, 유비쿼터스 센서 네트워크