IT Issues on Homeland Security and Defense

Kangbin Yim, Ilsun You

IT Issues on Homeland Security and Defense

Kangbin Yim[1] , Ilsun You[2+],

[1] 646 Eupnae, Shinchang, Asan, 336-745 Korea
yim@sch.ac.kr
[2] 214-32 Dongilro, Nowongu, Seoul, 139-791 Korea
isyou@bible.ac.kr
[+] corresponding author

Abstract. This paper surveys remarkable incidents that were related to the Homeland Security and Defense such as terrors, disasters and cyber-attacks and overviews the existing projects given by the department of Homeland Security and Defense of the US government. Through the overview, technological foundations in the projects are extracted and discussed. Additionally, this paper introduces a common framework, as an example, supporting the delivery service for RFID Tracking, Sensor Network, Video Surveillance and Image Screening, which are the major technological foundations in the Homeland Security and Defense. As providing an outline of the technological aspects of the Homeland Security and Defense, this paper is expected a reference for initiators of the related projects.

Keywords: homeland security, homeland defense, terror and disaster control, emergency readiness, and cyber threats

1 Introduction

IT convergence is a big topic of conversation these days. Through the convergence, the IT technologies have been applied to various traditional industries. The u-City and similar projects have merged IT framework into the traditional constructions and residential infrastructure and have connected the environment all around to the network. As the results, many private companies and even individual houses have incorporated ubiquitous sensor network connected to the Internet, large scaled intelligent video surveillance network has substituted the CCTV system, and the intelligent secure border wall has fielded sensors on the border fence between countries.

Even though the fundamentals of the Information Technologies are originated from military purposes, the traditional IT technologies developed and used in militaristic field were very confidential not more than twenty years ago. However, penetration of communication technologies into the public domain, such as the RF technologies and

network protocols for the cellphones and the Internet for example, had changed the situations in many ways.

Framework of communication is available totally in virtue of the standardization on its protocols and element technologies. However, standardization, in some aspects, makes security very difficult to be achieved. Because of the reason, another or several heavy layers of hardware or software are usually required to closely equalize the standardized results with the same quality of security to the confidential ones. Most of those layers are crypto based and mathematically approved and they are considered to be secure enough. However, lots of problems and subsequent accidents have been found on the real world implementations.

Recent advances and diffusions of Information Technologies as well as communication technologies also introduced a number of new services available to people in the public domain. To meet the requirement in the environment, many infrastructures in various industries and government organizations also have been connected to the Internet. Every local site in a gigantic class factory is monitored on the mobile phone in the public domain through the Internet. Videos for every common spot on the cruise ship can be delivered to public and live views on harbors, ports and docks are anytime available. Especially, many projects are recently involved to deploying unmanned surveillance and defensive systems even for nation-wide and military infrastructures. This means hackers can attack these infrastructures in such a way that was usually found in public domain.

Along with this IT convergence into the significant infrastructures, security problems and the defenses against the homeland are getting focused to consider. In case of the United States, the government reorganized many agencies to form the Department of Homeland Security after the September 11 terror attacks [3]. Other countries also have been focusing on the Homeland Security and Defense. Especially, many Korean researchers have insisted the government to prepare a strategic plan for Homeland Security and Defense because Korea is now a unique divided country in the world.

Even though the effort for the Homeland Security and Defense is getting focused, it could take too much time to have practical results and might miss the adequate time to adopt. Such as in the u-City projects, where there is a large gap in the viewpoints of the financial contributions between the IT industry and the existing industries.

2 Homeland Security and Defense

Homeland is defined as the physical region that includes the nation's possessions, territories, and surrounding territorial waters and airspace [1]. Homeland Security is defined as a concerted national effort to prevent terrorist attacks within the nation, reduce its vulnerability to terrorism, and minimize the damage and recover from attacks that occur [2]. Homeland Defense represents the protection of territory, sovereignty, domestic population, and critical infrastructure of a nation against external threats and aggression, or other threats [2]. Although Homeland Defense and Homeland Security are officially

defined separately and differentiated from each other as above, they are usually hsaconsidered interchangeable and the term Homeland Security and Defense (HSD) will be used in this paper to represent either or both.

As mentioned, HSD is based on the IT convergence to various existing industries because the industrial foundations are all components of the homeland. Major threats on the homeland components are terrors and natural or pollutional disasters. The terrors are unlawful violence or threat of unlawful violence to inculcate fear intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological [4]. There have been lots of terrors around the world for a long time. One of the most unforgettable terrors would be the September 11 attack in 2001, by which more than 3,500 people from more than 90 countries were killed and more than 60,000 million dollars was economically damaged. For the natural disasters, nobody could forget the recent two severe tsunamis that hit Japan and Thailand. The earthquake at Sichuan, China also killed more than 90,000 people and 370,000 people were wounded. For the pollutional disasters, smog in London, England and toxic chemical at Niagara fall, USA were most serious. The followings are the remarkable terrors since 2001 and disasters during this century.

Table 1. Remarkable terrors since 2001

when	where	how	casualty
07/2001	Colombo, Sri Lanka	airport bombings	43 /16 flights
09/2001	New York, USA	flight attacks	3,500 /$60B
04/2002	Jerba island, Tunisia	gas truck	20+ /$2M
11/2003	Istanbul, Turkey	Synagogue bombing	480 /$10M
03/2004	Madrid, Spain	train bombings	2000 /$20M
07/2005	London, England	subway bombings	756 /$100M

Table 2. Remarkable natural or pollutional disasters during century

when	where	why	casualty
10/1948	Donora, USA	smog	20+6,000
1940-52	New York, USA	toxic chemical	unknown
12/1952	London, England	smog	12,000
12/1984	Bhopal, India	toxic gas	2,800+200,000
05/2008	Sichuan, China	earthquake	90,000+370,000
12/2004	Andaman, Thailand	tsunami	18,000+
03/2011	Tohoku, Japan	tsunami	24,000+

Different from the disasters, worries about the location in HSD by terrors usually goes to the airports, seaports, plants or logistic flows. Even though these places are dealing with different flows or functions, it is common that the severity would be miserable if they were attacked. Therefore, the focus of HSD has been putted on the facilities on these places.

Besides the problems in HSD, the cyber threats are getting more threatening day by day. The cyber threats based on the terrorism in some cases may deliver more significant damages than practical terrors. People have had performance gain quad times per three years at half price, network bandwidth triple times per year in computing environment and now they gained the data transfer rate 90,000 times for 20 years and reduced the cost to 1% for 30years to process the same unit of data. This means that potential attackers can succeed a cyber-terror at a very low cost. Especially, 77DDOS attack in 2009 in Korea used well designed bot-net and left no footprint even though more than 60,000 personal computers were infected as an agent of the bot-net. In this situation, the DDOS attack is not the major problem and the damage would be more critical than expected because the framework is complete and the agent could equip any functions that were intended other than DDOS.

Table 3. Remarkable cyber threats during decades

when	from	to	how
1994	Personal/England	USA	PSTN-Internet
1998	worldwide	USA	complex
1998	unknown	India	miwOrm
1999	Yugo	Nato, USA	Mail bomb, virus
2000	unknown	Australia	SCADA
2001	China/USA	China/USA	Info warfare
2003	unknown	Korea+	Slammer
2009	unknown	Korea	77DDOS

3 IT Projects and Homeland Security and Defense

Department of Homeland Security (DHS) of the United States serves various activities and programs in such fields as Borders and Maritime Security, Chemical and Biological, Command, Control and Interoperability, Explosives, Human Factors and Behavioral Sciences, and Infrastructure and Geophysical. It also founded related entities such as Homeland Security Centers of Excellence, Homeland Security Studies and Analysis Institute, Homeland Security Advanced Research Projects Agency (HSARPA), and Office of National Laboratories (ONL) and published regulations, standards and references such as SAFETY Act, Science & Technology Standards, SECURE, S&T Snapshots, and Tech Solutions.

Especially in the Borders and Maritime Security field, dozens of IT based research projects have been issued. Summary of the projects is helpful to understand the state of the art IT researches and developments related to the HSD. The summary is as the following [5].

- Advanced Container Security Device (ACSD) Project is developing an advanced sensor system for monitoring containers' integrity in the maritime supply chain. The

ACSD is a small unit that attaches to the inside of a container to monitor all six sides and report any intrusion. If ACSD detects a symptom, it transmits alarm information through the MATTS to U.S. Customs and Border Protection.

- Marine Asset Tag Tracking System (MATTS) Project is establishing a remote, global communications and tracking network that works with Advanced Container Security Device. MATTS communicates security alert information globally through the use of radio frequency, cellular and satellite technology. In addition, the commercial shipping industry can track and monitor cargo as it moves through the supply chain.

- Advanced Screening and Targeting (ASAT) Project is providing an enhanced risk assessment through development of computer algorithms and software that will provide next-generation risk assessment and targeting tools to complement the CBP Automated Targeting System.

- Air Cargo Composite Container (ACC) Project is expanding upon the composite material developed in the Composite Container Project to determine whether it is effective in the air-cargo supply chain. The air cargo composite container must be comparable to existing aluminum containers and be interoperable with existing aircraft loading infrastructure.

- Automatic Target Recognition (ATR) Project is developing an automated imagery detection capability for anomalous content including persons, hidden compartments, contraband for maritime, land, and air cargo for existing and future Non-Intrusive Inspection (NII) systems.

- Border Detection Grid (BDG) Project is providing a grid of advanced sensors and detection, classification, and localization technologies to detect and classify cross-border movement. This technology will revolutionize border control by providing a way for a single Border Patrol officer to effectively monitor more than 10 miles of border.

- Border Officer Safety (BOS) Project is integrating technologies that will enable border-security and law-enforcement agents to more safely perform their mission. These technologies include Enhanced Ballistic Protection, Automatic Facial Recognition, Hidden Compartment Inspection Device, Pursuit Termination-Vehicle/Vessel Stopping, Covert Officer Safety Transmission System, Gunfire, Less-Lethal Compliance Measure for Personnel

- CanScan (CS) Project is developing a next-generation NII system that will be used to detect terrorist materials, contraband items, and stowaways at border crossings, maritime ports, and airports. These new systems may provide increases in penetration,

resolution, and throughput and will support marine containerized cargo as well as airborne break-bulk, palletized, and containerized cargo.

- Hybrid Composite Container (HCC) Project is developing a next-generation ISO composite shipping container with embedded security sensors to detect intrusions. Composites are stronger than steel, 10-15% lighter than current shipping containers, and are easier to repair.

- Secure Carton (SC) Project develops technology to detect any shipping carton tamper event and transmit an alert to authorities after it leaves the point-of-manufacture to the point that it is delivered in the supply chains. This project provides improved supply chain visibility, chain of custody, and security.

- Secure Wrap (SW) Project provides a transparent, flexible, and tamper-indicative wrapping material to secure and monitor palletized cargo after it leaves the point-of-manufacture to the point-of-delivery in the land, maritime and air-cargo supply chains.

- Sensors/Data Fusion and Decision-Aids (SFDA) Project develops systems to enable law enforcement officers and commanders to have full situational awareness, enabling effective decision making and execution in complex and dynamic operational environments.

- Sensors and Surveillance (SS) Project develops and demonstrates visual and non-visual technologies for monitoring the maritime border. The project includes the technologies such as Affordable Wide-Area Surveillance, Advanced Geospatial Intelligence Technical Exploitation, Port and Coastal Radar Improvement, Small Boat Harbor Surveillance Study/Pilot, Inland Waterway Maritime Security System.

- Situational Awareness and Information Management (SAIM) Project provides information management technology to quickly identify threats at the maritime border and to provide required information to decision makers and security forces.

- Supply Chain Security Architecture (SCSA) Project maps the international supply chain including point-of-stuffing, port-of-entry, shippers, CBP, foreign Customs, and container manifests to provide DHS the framework to incorporate near-term and future container-security technologies into supply chain operations.

Throughout the survey of the projects summarized above, technological aspects or foundations are categorized into two main issues including RFID Tracking and Sensor Network (RTSN), and Video Surveillance and Image Screening (VSIS) as shown in fig. 1. In the RTSN field, interface specification, integrating protocols, power management, routing algorithms, and location privacy problem are considered. In the VSIS field, integrating protocols, object extraction, relation and tracking, image distribution, interoperability, privacy masking and restoration are considered.

For the RTSN, interface includes analog and digital specification of the sensor modules. Analog interface is based on either current loop or voltage level, which is less than several mA in peak and TTL level or CMOS level, respectively. Integrating protocols are related to interoperability between sensor modules and several frames are defined for control, status and data. Power management is important because sensor modules used in HSD framework are almost wireless ones and it is sometimes involved with the routing algorithm, which delivers sensing information all around the sensor modules and unwanted module should be awaken to relay others' information. Location privacy can be achieved by encryption or nebulosity. Encryption and nebulosity cause much overhead respectively in computing and bandwidth and need to be traded off.

For the VSIS, protocols to transfer image information are different among devices and need to be converged. The VSIS is highly involved with image information and object extraction or sometimes object tracking in a video is required to enhance intelligence of the system. To share the information, the distribution function is essential though the devices usually don't support it. Sharing of the image information sometimes causes privacy invasion problem and a privacy masking policy is required. The privacy mask also needs to be stripped in case of criminal investigation.

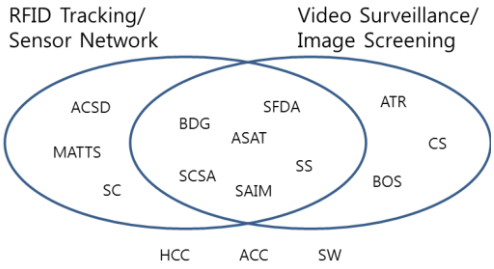

Fig. 1. Technological aspects or foundations are classified into two categories: one is for RFID Tracking and Sensor Network (RTSN) and the other for Video Surveillance and Image Screening (VSIS). Some projects are in RTSN, some in VSIS and the others in both.

4 Major Topics in Homeland Security and Defense

As mentioned, RTSN and VSIS are major research topics for the HSD. Although the features and characteristics of these categories are far different, their frameworks and architectures to acquire and share the related information are similar to each other. The major differences are on the endpoint interfaces and client software organizations. However, convergence of these differences into a coherent architecture leads a common

framework sharable as shown in fig. 2. This chapter introduces a reasonable architecture of the common framework for RTSN and VSIS.

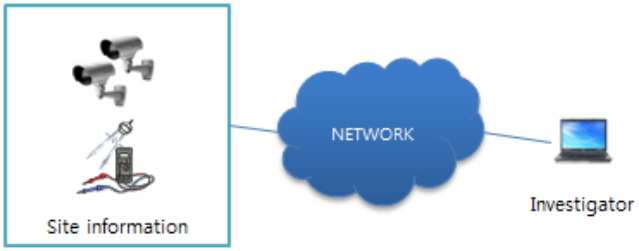

Fig. 2. Although the features of RTSN and VSIS are far different, their frameworks are similar to each other and the differences on the endpoint interfaces and client software organizations can converge into a unique framework to share.

During this couple of decades, video cameras are digitalized and improved to become modernized for the integrated video surveillance system. The video surveillance system originally has been regulated to provide a closed security channel monitoring public violence such as illegal car parking, illegal waste dumping for where there is no security staff hired. However, the communication society required for more digitalized camera connections to many different fields including farmlands, factory assembly lines or disaster sites or even borders between countries.

Even though the traditional CCTV was for closed channel as mentioned above, recent hot issue on the video surveillance system is to provide an integrated framework that is compatible with heterogeneous video formats and protocols along with supporting multiple cameras and clients. During the development of the video surveillance systems, researchers have contributed many efforts to a better protocols and compression algorithms to provide best service connections. However, that approach was considered a failure when they started to connect multiple cameras and multiple clients in an integrated network. The existent performance and bandwidth of a networked camera have proved that they are limited in the number of client connections to a camera. Even more, management and security problems were arisen where the cameras have been installed at remote places and isolated from the regular update and secure environment. Because of the reasons, the centralized management system (CMS) for multiple cameras and multiple clients became required to be deployed within a secure network as a proxy server and integrate the multiple cameras and clients [8].

For a usual CMS, it is deployed along with a new deployment of a same type of new multiple cameras for a new site. However, to integrate the existing multiple cameras or sites, a new adaptation mechanism is required for different types of cameras from different vendors [9]. Several frontier projects supported by the government yet replaced hundreds of existing cameras each because of the incompatibility. Just a small site seems

reasonable to replace them as well as do for sites that have one type of camera dominantly deployed in number. However, new software architecture is required to seamlessly integrate different types of cameras for a globalized intelligent surveillance network, which is required these days.

Originally, networked cameras have been incorporating their own individual protocols and providing dedicated API libraries to give accessibility to users. These protocols were usually designed based on simple socket connections. For this kind of cameras, client software needs to implement all the sequences to request the images directly to the server.

Socket-based individual protocols required to much overhead for client software developers. Subsequently, the architecture of the network camera has changed for easy connections. Therefore, comparatively new models has incorporated HTTP based web server for connection and control and RTP facilities for video streaming [7]. In general, the HTTP is a set of rules for transferring files including text, images, sound, video, and other multimedia files. Because the networked camera deals with several different media, this transfer method has been applied to networked camera communication services.

The HTTP based protocols requires for client software developers only to organize a text based script to connect to the server and enables them easy to develop. However, the message formats for the script were still diverse because the network camera manufactures are quite different in the way of accessibility, control features and image compress methods, such as JPEG, MJPEG, MPEG, and Wavelet. Because of the incompatibility between client software, the administrator should have managed each site by running different client software. Additionally, each client from different manufacture had its own independent modules for connection and decoding, there were much overhead and inflexibility on the user platform running multiple clients. As the result, the government or a large scaled organization has found much difficulty to manage and access different network cameras in remote sites in parallel to servicing the videos for massively multiple users [6].

Generally, camera manufacturers provide API libraries to encourage client software development. Some of the libraries have a part of portable modules for both connection and decoding, which are dynamically inserted into client software. It makes time-to-market very short because several lines of script can assess the dedicated cameras. It is easy to construct a CMS and also helpful when the CMS integrates multiple cameras even from different manufactures if they have detailed specification for the software interfaces only if the server needs to be connected from just one client. In this case, client script simply embeds portable modules that were already published on the server for each camera then the modules will be downloaded and executed on the client platform.

When multiple clients want to connect to the same camera, problems arise. As mentioned, effectively only one connection is allowed to a networked camera. To overcome this limitation, the CMS server needs to distribute the video stream that was gathered from a camera to multiple clients. In this situation, it is very difficult for the CMS to provide the same functionality as was provided on various cameras because heterogeneous connection protocols and media formats are transacted between the CMS

server and clients in this approach. Therefore, an architectural framework should be designed to provide a flexible incorporation of various cameras for multiple users.

Instead of emulating camera functionality on the CMS, a unified connection protocol could be designed between the CMS server and clients and an integrated portable module could be distributed to the client software. The CMS server can only be responsible for connection to cameras using connection modules and bypass all the media information from cameras to multiple clients. It is essential for camera manufacturers to provide a separated set of connection and decoding modules for the CMS server and the clients, respectively. In this approach, the CMS server plays a role as a media switch. Even though the CMS server needs to brew connection modules if camera manufactures didn't provide them, it would be simpler than developing a number of camera emulators.

Analyzing basic architecture of the network cameras, their APIs, image compression algorithms and protocols may confuse in many ways. However, it is required to analyze, evaluate, classify the existing features and design a unique coherent architecture for heterogeneous environment.

Several considerations are especially required on designing the decompression module for clients. For the networked camera based on the JPEG compressed images the client could completely decompress an image independently. However, MPEG or modifies Wavelet based images are transacted by components independently from key frame (I-Frame) to delta frame (P-Frame) only if some changes occur on the information. This means that if client didn't received any key frame from the camera, client itself is unable to decompress delta frame image. Therefore, this integrated client need to receive a key frame and keep it until the delta frame is resolved. For the sensor information, the parsing module is prepared. This module restores the data frame into the original format of sensor information.

The CMS server is designed to have six separated functional stages. Internal structures and information flows in the server are shown in fig. 4. For a connection request, it is issued only when a client asked for the camera. Although this type of connection minimizes number of simultaneous connections, it takes too much delay for connection setup. Instead, pre-connection sets up possible connections to cameras and maintains them.

Queuing is required between the server and the client software for each connection to support analogous service. The number of buffers for queuing is determined by the policy of the jitter management. In case of multiple clients to ask for the same video stream from a camera, the video information is copied to multiple queuing buffers on the distribution stage. On the processing stage, several selective functions are provided. These functions include frame rate scaling, privacy masking and encryption. The frame rate scaling is an alternative for the jitter management on the queuing stage. Privacy masking in this stage is post-compression privacy masking and it is sometimes very difficult and gives too much overhead because it needs to find adequate marker codes. Rectangular masks are only possible as well.

Some connection modules are prepared for sensor modules. According to the connection specification of the sensors, these connection modules are designed as a virtual camera connection.

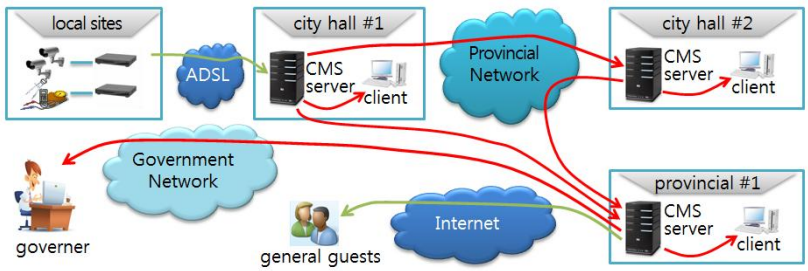

Fig. 3. Overall architecture including a common framework and equipment supports heterogeneous information such as video stream, image shot and various types of sensor data

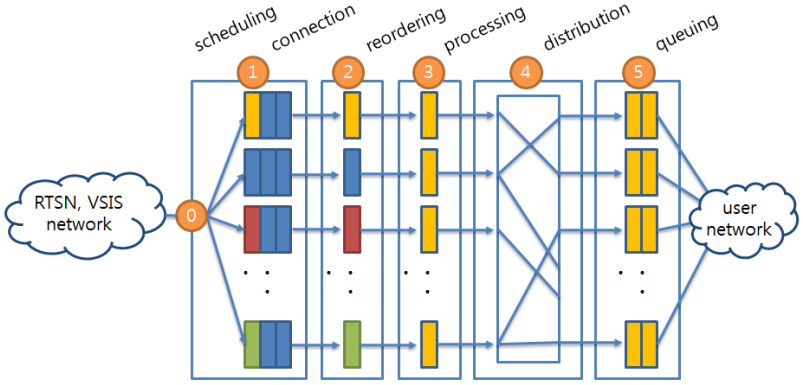

Fig. 4. Server software is composed of several stages for different functions including scheduling connections, buffering and reordering packets, processing image or sensor information, and distributing them to multiple clients.

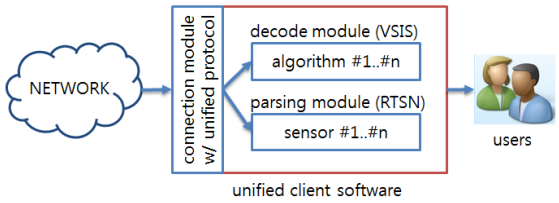

Fig. 5. Client software is composed of three different function modules: connection module for unified connection protocol, decode module for decompress or restoration of the images or objects, and parsing module for sensor information.

5 Conclusions

This paper surveys existing projects, technological foundations in the Homeland Security and Defense and introduces a common framework supporting delivery service for RFID Tracking, Sensor Network, Video Surveillance and Image Screening. Because almost every infrastructure as a component of the homeland is getting connected to the Internet, existing cyber threats are potentially possible to be applied to the framework of the Homeland Security and Defense. If these kinds of threats are tried and realized by possible terrorists, severity of the relevant attacks would be more than that of the physical terrors and the range of the affection would be worldwide. Because of the reason, considerations on the countermeasures to the vulnerabilities and attacks to the infrastructure of the Homeland Security and Defense are required. Especially, research topics required in near future need to be carried on shortly to keep the homeland security infrastructure safer. Several major ones of these topics are as the following.

- Multiple privilege level support for access control to RTSN and VSIS data
- Key management framework for multiple privileges and privacy masking/restoration
- Dynamic privacy masking technology to mask on compressed data, images or videos
- Intelligent object extraction and masking algorithm
- High speed object extraction and tracking algorithm
- Synchronization of multiple heterogeneous data sets
- Secure primary and secondary backup of the integrated data
- Indexing and retrieving policy for image or sensor data
- Real-time support for sensor information

Especially, researches on the dynamic privacy masking, the privacy mask restoration based on multiple privilege levels, and the secure secondary backup storage are now on the way, related to the framework introduced in chapter 4.

Acknowledgments. This work (Grants No.00043599) was supported by Business for International Cooperative R&D between Industry, Academy, and Research Institute funded by Korea Small and Medium Business Administration in 2010.

References

1. T. Michael Moseley: Homeland Operations. Air Force Doctrine Document 2-10, pp.9--10 (2006)
2. Walter L. Sharp: Homeland Security. JP 3-27. http://www.fas.org/irp/doddir/dod/jp3_27.pdf (2007)
3. Angus Martyn: The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September. Australian Law and Bills Digest Group (2002)

4. Charles L. Ruby: The Definition of Terrorism. In: Analyses of Social Issues and Public Policy, pp. 9--14. (2002)
5. Department of Homeland Security, http://www.dhs.gov/index.shtm
6. The Best Source for Digital Video and Network (IP) Security Products. http://www.cctvsentry.com/
7. Network camera developments enable live web imaging. White paper, Axis (1999)
8. IKebe, Oqawa, Hatayanma: Network camera system using new home network architure with flexible scalability. In: International conference on ICCE2005, pp. 151--152. (2005)
9. Kyungroul Lee, Kangbin Yim, Mohammad Mikki: A secure framework of the surveillance video network integrating heterogeneous video formats and protocols. Submitted to be published on the Journal of Computers and Mathematics with Applications.
10. Kyungroul Lee, Kangbin Yim: Safe Authentication Protocol for Secure USB Memories. In: Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA), Vol.1, No.1, pp.46--55. ISYOU (2010)