

Ubiquitous Video Surveillance Service with Secure Forwarding Agents

Te-Chih Wang, Chia-Hui Wang*, Ray-I Chang, Jan-Ming Ho[†]

Dept. of Engineering Science & Ocean Engineering, National Taiwan University, Taiwan

**Dept. of Computer Science & Information Engineering, Ming Chuan University, Taiwan*

[†]Institute of Information Science, Academia Sinica, Taiwan

{d95525010, rayichang}@ntu.edu.tw, wangch@mcu.edu.tw, hoho@iis.sinica.edu.tw

Abstract—Video surveillance systems have been playing an important role to protect lives and assets of individuals, enterprises and governments for decades. Due to the prevalence of wired and wireless access to Internet, ubiquitous video surveillance (UVS) service could be fulfilled to provide diversified surveillance services. In this paper, forwarding agents of multicast agent (MA) and super agent (SA) with security protection via Diffie-Hellman key exchange algorithm are proposed for UVS, so forwarding agents can provide surveillance video streaming service with scalability, ubiquity and privacy on the public Internet. FEC is also applied for reliable surveillance-video multicast to preserve the playback quality of UVS both on Internet and 802.11 Wireless-LAN. The experimental results from the deployed UVS test-bed with Wi-Fi Internet access demonstrate the effectiveness of the proposed schemes for UVS.

Index Terms—video surveillance, multicast, Diffie-Hellman key exchange algorithm, FEC.

I. INTRODUCTION

VIDEO surveillance services have been active for decades to protect lives and properties of individuals, enterprises and governments such as homeland security, office-building security and traffic surveillance on highways. Due to the technology advancements in digital media compression, computer computation and wired/wireless communications, video surveillance has been led to wide deployment over Internet to provide ubiquitous video surveillance (UVS) services [1][2][3] with more flexibility and easier usage than ever. Besides, value-added and diversified UVS services can be produced by integrating with other full-fledged applications on Internet.

However, the architecture of Internet and most of the media codecs applied on delivered packets are open to public, not only the reliable delivery for surveillance videos is required to achieve playback quality of UVS, but the privacy protection of sensitive surveillance videos should be also protected.

In this paper, we propose to apply forwarding agents of multicast agent (MA) and super agent (SA) to provide scalable, ubiquitous and reliable UVS. To firstly achieve scalability

The work was partially done while the author was visiting the Institute of Information Science, Academia Sinica, Taiwan in 2007 and partially supported by National Science Council, Project No. NSC 96-2218-E-002-029, Taiwan..

while we need one-to-many service discipline, surveillance videos are delivered via multicast to reduce the burden on Internet and servers. However, most of the Internet routers turn off forwarding of multicast packets to avoid flooding of multicast traffic. Therefore, forwarding agents can apply unicast tunnel to forward multicast surveillance videos from one multicast island to another.

Secondly, forwarding agents are also applied to extend video surveillance services to private networks achieve ubiquity for UVS. Thirdly, to achieve privacy protection for sensitive video surveillance content, we further apply Diffie-Hellman key exchange algorithm to produce common private encryption-key for encrypting each surveillance video delivering between forwarding agents through public Internet.

Though conventional technologies of VPN and IPSec can also achieve Internet access in private networks and security protection respectively, the forwarding agent can further provide application-level services without any specific hardware support.

Finally, we apply forward erasure correction (FEC) to multicast video packets to preserve playback quality of UVS, not only because the prevalent 802.11 wireless-LAN doesn't guarantee the QoS of multicast delivery [7][8], but also due to the unreliable unicast tunnel between forwarding agents. Thus, the proposed schemes mentioned above can achieve reliable UVS through wired/wireless Internet access.

The rest of this paper is organized as follows. In Section II, we present the proposed system and architecture for UVS, called OpenIVS[5] (Internet Video Surveillance service with Open-source) and describe how the proposed architecture to achieve scalability, ubiquity and reliability for UVS on Internet. In Section III, we propose secure forwarding agents to provide privacy protection for the surveillance videos of UVS. The performance results of quality of UVS via the experiments on OpenIVS test-bed are presented in Section IV. Finally, Section V concludes this paper.

II. SYSTEM ARCHITECTURE AND PROTOCOLS

OpenIVS logically comprises three components to provide ubiquitous video surveillance services. The first component is the customary video surveillance services closely related to end-users. The second component is the multicast agent (MA) to extend customary video surveillance services within

multicast islands. The last component is the super agent (SA) to basically connect customary video surveillance within private networks over the Internet. Fig. 1 shows the main architecture of our internet video surveillance platform. The detail description of each subsystem component will be shown in following sub-sections.

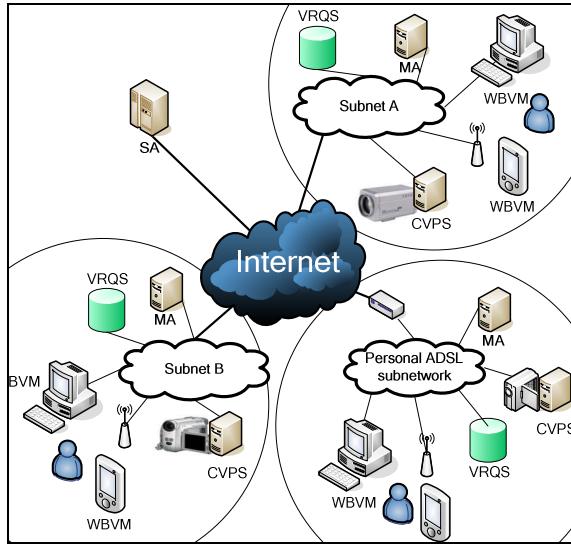


Fig. 1. Architecture of OpenIVS.

A. Customary Video Surveillance Services

Customary video surveillance services [3][5] are basic video surveillance services with consideration of scalability and reliability. They are provided by 3 kinds of different subsystems: Compressed Video Pumping Server (CVPS), Video Recording and Querying Server (VRQS), Web Browsing Viewer and Manager (WBVM). These subsystems are listed and summarized below:

CVPS:

- Compress the captured video from surveillance camera.
- Attach FEC packets to compressed video packets to achieve reliable service
- Then multicast video packets with FEC packets to network to achieve scalable and reliable service

VRQS:

- Record surveillance videos via a file system.
- Provide query interfaces for reviewing the stored video

WBVM:

- Provide users' interfaces to view surveillance videos.
- Provide administration functions within above-mentioned subsystems and agents, such as the settings of CVPS, the information of SA and the mapping information between a CVPS and its MA.

However, these subsystems can only provide domestic video surveillance service without consideration of ubiquity on Internet. We will discuss how to achieve ubiquity for UVS via MA and SA in following subsections.

B. Multicast Agent

MA are used to connect multicast islands to help UVS to achieve ubiquity. An operation example of MA is shown in Fig 2. There is a MA located in subnet A, which is denoted as sMA(source MA), and dMA is responsible to receive the multicast video from CVPS and then forwarding it to other MAs, said destination MAs(dMA), in different subnets.

Once external users located in different subnet B and C want to watch the same surveillance video from subnet A, two dMAs, which are respectively located in subnet B and C, will take the responsibility to receive the surveillance video forwarded from remote sMA in subnet A. Then, these two dMA will re-multicast the received video packets for the external users in subnet B and C.

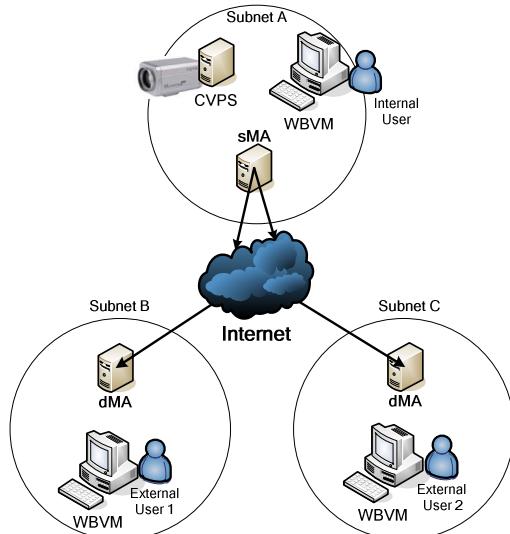


Fig. 2. Operation example of MA.

Above-mentioned sMA and dMA are different functional terms from MA. They are usually implemented as one together. The packet sample of surveillance video delivered between sMA and dMA is shown in Fig. 3. Therefore, domestic video surveillance service can be extended to remote subnets via proposed MA.

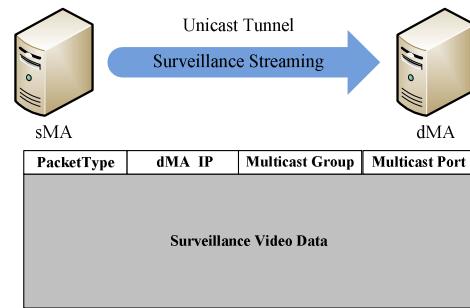


Fig. 3. Unicast packet sample from sMA to dMA

However, domestic video surveillance services may be located in private networks. MAs with functions of sMA or dMA could also be located in private networks. Then the challenge is how to extend domestic private surveillance services in private networks to achieve ubiquity. In the following sub-section, we will give detail description about

how to apply super agent (SA) to achieve UVS's ubiquity no matter whether the sMA or dMA is located in private network.

C. Super Agent

Since the NAT technology [9] has been used widely to provide Internet access from private networks. In our OpenIVS, for example, a sMA is hard to receive service requests while it is located behind a NAT device. Thus, we propose super agent (SA) in OpenIVS to achieve ubiquity to forward surveillance videos for MAs located in private networks. SA serves as a centralized proxy to solve this NAT traversal problem for OpenIVS.

This so-called super agent is also responsible to not only maintain the administrative information of MAs such as their configuration and connection data, but also provide video surveillance point mapping of which CVPS multicasts the request surveillance videos and which sMA (i.e. sMA) that the dMA can contact for forwarding this surveillance video via the sMA.

Therefore, SA is another kind of forwarding agent to forward surveillance video packet while dMA is located in private network. Besides, SA will also establish command link with sMA and dMA respectively and forward command request of service between them. To efficiently achieve ubiquity for UVS via proposed forwarding agents, we discover 4 kinds of different video forwarding paths listed below from sMA to dMA and elaborate on how to forward surveillance video which external users request.

(1). Public network to public network:

If a CVPS's sMA and its external user's dMA both belong to public networks, sMA and dMA obviously have their own real IP addresses to easily communicate with each other. At the beginning, sMA will join the same multicast group as CVPS to receive surveillance video packets. And then, sMA encapsulates the received packet content with a header (as shown in Fig. 3) and unicast them to dMA, which includes multicast group address and multicast port number in front of each multicast packet's content. Finally, while dMA receives these unicast packets, it de-encapsulates the packets and multicast them according to the header information to dMA's subnet. Then, all external users, who are locate in the same subnet as dMA, can watch the surveillance video from sMA.

(2). Private network to public network:

This situation happens when a CVPS's sMA and its external user's dMA belong to private and public networks respectively. Communication procedure of forwarding video packets and command requests between these two MAs is the same as sMA and dMA are both located in public networks. That's to because dMA is located in public network and the forwarding video packets can be sent to it without troubles, no matter whether the sMA is located in public or private network. Therefore, the communication procedure while dMA is located in public network is shown in Fig. 4 and the operations are listed as following:

- First of all, dMA sends a multicast-traffic request message

(MT_REQUEST) to SA by a pre-created link.

- Secondly, according to the information contained in MT_REQUEST, SA forwards the message with some extra information appended to sMA. The extra information contains dMA IP address and whether dMA is located in public or private network. In this case, dMA is in public network.
- Finally, sMA directly sends the surveillance video to dMA by unicasting, and dMA multicasts them to its network.

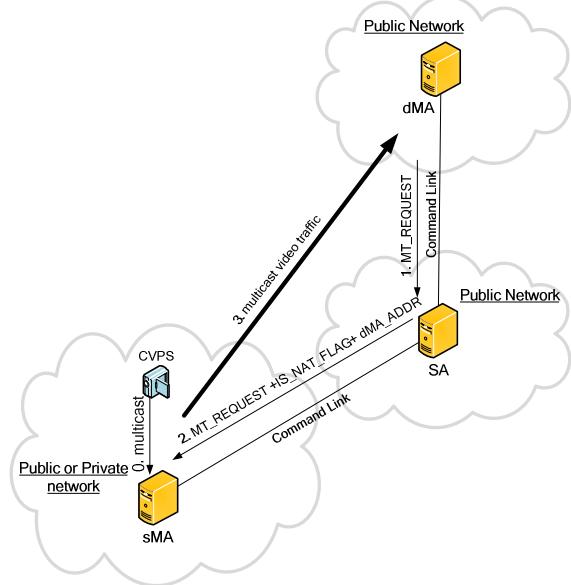


Fig. 4. Communication procedure while dMA is in public network.

(3). Public network to private network:

If CVPS's sMA and external user's dMA belong to public and private network respectively, dMA cannot receive packets from sMA directly. Hence, SA is applied to serve as an intermediate relay between sMA and dMA to re-forward packets. While dMA is located in private network and its user issue the first request for remote surveillance video, dMA has to send a multicast-traffic request message via SA to sMA. Then sMA starts to transmit the multicast surveillance video through SA to dMA by unicasting. As the usual, dMA then multicasts the received packets to users and users belong to the private network can watch the surveillance videos from remote networks.

(4). Private network to private network:

If a CVPS's sMA and external user's dMA both belong to private networks, communication procedure of forwarding video packet and command requests between these two MAs is the same as the situation mentioned above, said "*public network to private network*". Thus, we present the communication procedure in Fig. 5 while dMA is located in private network. And the operations are shown as following:

- First of all, dMA sends a multicast-traffic request message (MT_REQUEST) to SA through a pre-created link.
- Secondly, SA forwards the multicast-traffic message with some extra information appended to sMA. The extra

information contains dMA IP address and whether dMA is located in public or private network. In this case, dMA is in public network.

- Then, sMA sends the surveillance video packets to SA by unicasting.
 - Finally, SA redirects the surveillance video packets to dMA, and dMA multicasts them to its network.

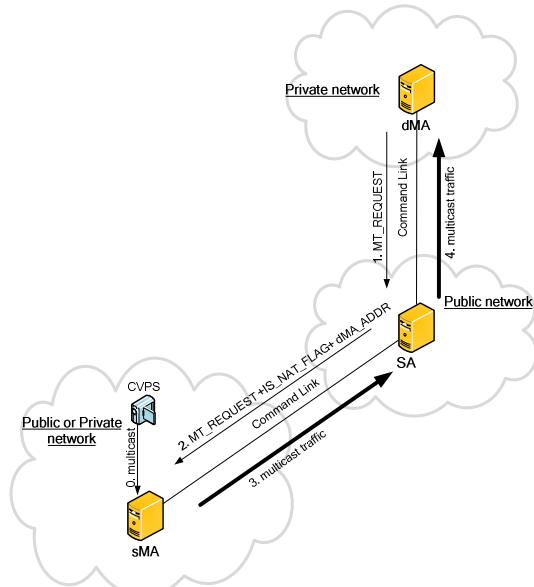


Fig. 5. Communication procedure while dMA is in private network.

III. SECURE FORWARDING AGENTS

Due to the scalable, ubiquitous and reliable abilities for UVS on Internet have been proposed in last section, we also take account of the security issues. As mentioned earlier, SA is a centralized architecture and contains all the important information of UVS. Malicious users can be prevented by authentication from accessing valued information of UVS. However, surveillance video should also be protected due to its transportation over the public network, Internet. Thus, we are going to focus the security issue about surveillance video delivered between SA and MAs in this section.

Considering security strength and real-time constraint of the surveillance videos, we chose well-known symmetric cryptography, AES [10], as our encryption and decryption algorithm to protect sensitive surveillance video content in forwarding. Besides, we also apply Diffie-Hellman key negotiation algorithm (DH) to negotiate an encryption key, and then periodically change encryption key [11] to boost security strength.

In OpenIVS, our privacy protection for surveillance video will be focused on how to furnish the encryption key negotiation. Once the key negotiation has been done, surveillance video can be transmitted by the procedure we mentioned in section II. The key negotiation can be separated by two parts: MA to SA and sMA to dMA. Then, the detail description of key negotiation procedures about these two parts are shown at following.

Fig. 6 shows the key negotiation procedure between MA (i.e. sMA and dMA) and SA. By exchanging MA's and SA's public key, MA and SA then negotiate a common secret key for privacy protection for the surveillance videos forwarded between MA and SA.

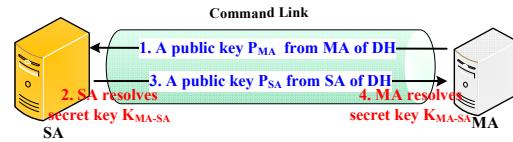


Fig. 6. Key negotiation between MA and SA

Besides, before the surveillance videos are directly transmitted between sMA and dMA, they need to negotiate a common secret key. Fig. 7 presents the key negotiation procedure between sMA and dMA via SA. While the key negotiation procedure is done, sMA then directly send the surveillance video to dMA as shown in Fig. 4.

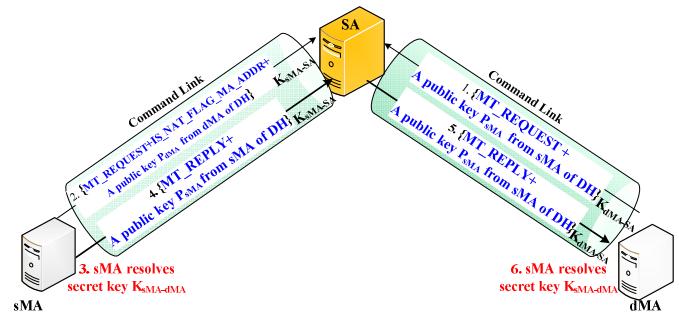


Fig. 7. Key negotiation between dMA and sMA

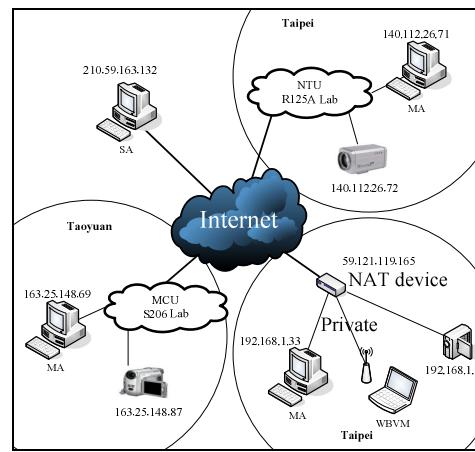


Fig. 8. Experimental environment

IV. EXPERIMENTS AND PERFORMANCE RESULTS

We also did some experiments to demonstrate not only the impact of video playback quality while we apply AES security mechanism to encrypt/decrypt the surveillance videos in H.263 compression, but also the reliability of applying FEC in OpenIVS. Fig. 8 shows the experimental environment. There are three multicast islands, such as NTU R125A lab which is located in the laboratory of national Taiwan University in Taipei city, MCU s26 lab which is located in Taoyuan county, and a private network which is also located in Taipei. Each of

these multicast islands has a MA to forward their surveillance video. Besides, a client WBVM located at the private network would display these surveillance videos from surveillance spots in these multicast islands.

Fig. 9 shows the impact of sending rates and receiving rates while applying privacy protection into OpenIVS. The sending rates on CVPS and receiving rates on WBVM both ranged between 14.5 to 15 fps. We could see that the average sending and receiving rates are quite similar. And the surveillance video is also smoothly played on WBVM. That means we successfully connected these three multicast islands without influencing the playback quality by using proposed forwarding agents of MAs and SA while the UVS architecture is applied.

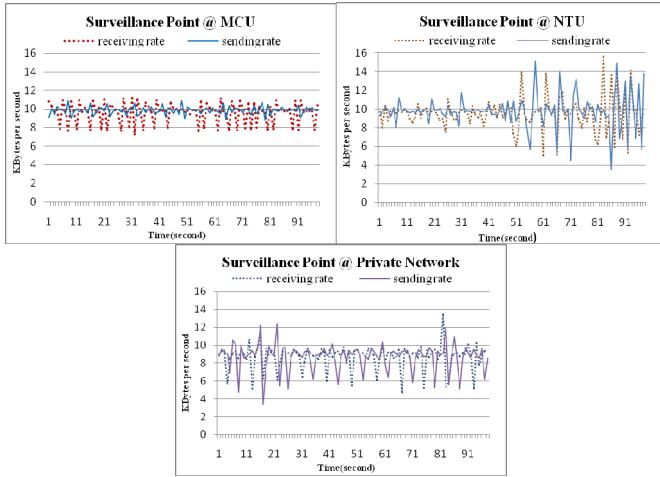


Fig. 9. Sending and receiving rate of each surveillance point

Then, we compare both the sending rates and receiving rates at MCU while the privacy protection mechanism with AES encryption is applied on forwarding agents and the results is shown in Fig. 10. The results also point out the security protection we applied on forwarding agents does not degrade the transmission rate (i.e. the average transmission rates are almost equal) and we can securely deliver the surveillance video on Internet without affecting the playback quality.

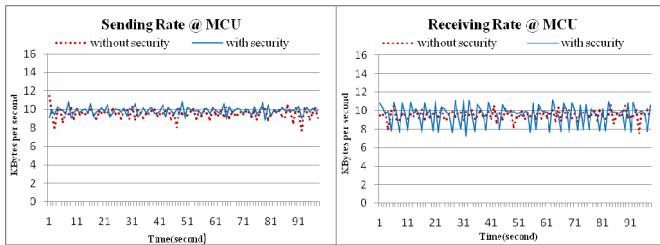


Fig. 10. Sending rate and receiving rate of weather the security mechanism is applied

Finally, because it is hard to evaluate the performance of FEC applied on OpenIVS, we did a simulation to measure the reliability that can be achieved by applying FEC on OpenIVS. The simulation is done by sending 5000 multicast packets with sending rate 225kbps, each packet contained payload size of 512 bytes, and 25 FEC packets were added for every 50 video

surveillance packets. In the FEC simulation on the private network with Wi-Fi access point, 103 packets were totally lost at receiver after transmission. Packet lost rate reached to 2.05%. While applying FEC during the transmission, all lost packet were recovered at receiver. Packet lost rate can be reduced to zero. According to the simulation results, FEC is very helpful to recover lost packets for UVS on Internet to preserve playback quality, especially on prevalent Wi-Fi wireless environment.

V. CONCLUSION AND FUTURE WORK

In this paper, a ubiquitous surveillance system has been proposed and implemented. The proposed architecture has the ability to efficiently integrate independent surveillance systems that locate in public or private networks. Besides, security issue is considered in the proposed architecture. We also demonstrate some experiments to evaluate the effective OpenIVS by good performance results. In the future, we are going to extend multicast agent with support of load sharing, to efficiently reduce loading to a popular sMA and its network.

REFERENCES

- [1] A. C. M. Fong and S. C. Hui, "Web-based intelligent Surveillance System for Detection of Criminal Activities," Journal of Computing & Control Engineering, vol. 12, no. 6, page(s): 263-270, Dec. 2001.
- [2] L. F. Liang and S. Y. Yu, "Real-Time Duplex Digital Video Surveillance System and Its Implementation with FPGA," Proc. Of Int. Conf. on ASIC, page(s): 471-473, 2001.
- [3] J.M. Ho, R.I. Chang, J.Y. Juang, C.H. Wang, "Design and Implementation of a Web-Based Surveillance System using Internet Multicast Communications," SoftCOM 2000, IEEE.
- [4] Chia-Feng Juang, and Chia-Ming Chang, "Human Body Posture Classification by a Neural Fuzzy Network and Home Care System Application," IEEE Trans. Syst., Man, Cybern, vol. 37, pp.984-994, Nov. 2007
- [5] Chia-Hui Wang, Ray-I Chang, Jan-Ming Ho, "An Effective Communication Model for Collaborative Commerce of Web-based Surveillance Services," E-Commerce, 2003. CEC 2003. IEEE International Conference on, 24-27 June 2003, Page(s): 40 -44.
- [6] OpenIVS, Available at: <http://OpenIVS.dyndns.org>
- [7] J. Xie, A. Das, S. Nandi, A. K. Gupta, "Improving the reliability of IEEE 802.11 broadcast scheme for multicasting in mobile ad hoc networks," Communications, IEE Proceedings- Volume 153, Issue 2, 1 April 2006 Page(s):207-212.
- [8] Chong-Wei Bao, Wanjiun Liao, "Performance analysis of reliable MAC-layer multicast for IEEE 802.11 Wireless LANs," Communications, 2005. ICC 2005. 2005 IEEE International Conference on Volume 2, 16-20 May 2005 Page(s):1378 - 1382 Vol. 2.
- [9] RFC 3489, STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).
- [10] National Inst. Of Standards and Technology, Advanced Encryption Standard, Federal Information Processing Standard 197, Nov. 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [11] Chia-Hui Wang, Mei-Wen Li, Wanjiun Liao, "A Distributed Key-Changing Mechanism for Secure Voice Over IP (VOIP) Service," IEEE 2007 International Conference on Multimedia & Expo (ICME 2007), July 2-5, 2007, Beijing, China.