Research Proposal for CERIAS RFP2000:

# Adaptability in Multimedia Data Security

**Bharat Bhargava: Principal Investigator**
Department of Computer Science
Purdue University
West Lafayette, IN 47907
bb@cs.purdue.edu
765-494-6013

I intend to explore possibilities for external funding of the project. I have read the policies for CERIAS-funded projects and agree to abide by them. I plan to seek funding from National Science Foundation, Army Research Lab and ARPA. I plan to submit a proposal in Fall 2000.

# Contents

# 1 Introduction

Distributed multimedia systems are used to store and process information whose disclosure, alteration, or unavailability would have significant economic or strategic costs. Military documents, geographical terrains, global position and routes of troops, location of enemy positions and supply lines are examples of multimedia data. In addition, web data relating to B2B commerce (design of products, contracts, pricing charts) and research reports of investment firms are part of digital library/multimedia data [5, 6]. Among the factors that affect the distributed applications are various anomalies, which we classify into two categories: operational failures and functional limitations. Operational failures refer to system crash due to security check failure. Functional limitations refer to those caused by resource constraints such as cyber attack, network congestion, and system overloads. This includes intentional attacks due to intrusions and attacks on security and privacy. We propose to study adaptable solutions to deal with the problems associated with these anomalies. Due to security violation in a distributed system, graceful reconfiguration is needed. To allow dynamic reconfiguration, we need to design systems that have the infra-structure in terms of algorithms and their respective data structures to support switching to new configurations. The challenge lies in identifying and responding to anomalies, in designing protocols for correct switching between modules without halt in processing, and in determining the correct set of security checks to run in a given situation.

Active network [1] is a paradigm for providing customized network service to the applications. In this environment, the packets can carry active programs within the packet to enable specialized processing on them [13, 12]. Active networks allow application programs to inject specific programs to any intermediate nodes (routers). These active programs need to be executed securely to avoid any intentional or unintentional breach of system security policies. Active networks provide the flexibility for the application program to modify the default services a router can provide to suit its specific needs. Therefore it has the potential to provide the application-level QoS at the transport or network layers.

One application of active techniques is video transcoding [3]. The emerging applications will contain multimedia data such as video and audio data. How to provide secure multimedia data processing capabilities within these new service architectures is a challenging issue. Currently available general purpose mobile languages and virtual machines such as Java provide some built-in security mechanisms such as sand-box execution model [15]. A multimedia system needs to provide the same data at different level of security to different users based on the content (semantics) of the data and the profile of the users. When the video data is routed outside the sender's domain, the security level need to be increased to protect the intellectual property right. In contrast, if the video clip is a commercial, then the least security level can be used throughout the whole multicast tree. Active networks paradigm provides mechanisms to achieve this kind of adaptable security [4].

# 2 Statement of Problem and its Importance

The challenges of multimedia data encryption come from two facts. First, the sizes of typical multimedia data are large (for example, the size of a two-hour MPEG-1 video is about 1

GB). Second, multimedia data needs to be processed in real time (for example, the data rates of MPEG-2 videos range from 4 MB/sec to 10 MB/sec). Processing vast amount of data in short time puts great burden on video codec, storage space requirements and network communications. Heavy-weight encryption and decryption algorithms (during or after encoding phase) will aggravate the communication/storage and increase the latency.

Multimedia data security is an important issue in both traditional and emerging applications. For example, in video-on-demand and video conferencing applications, it is imperative that only those who have paid for the services can access the data. A popular method to secure multimedia data is to treat this data as a binary file and encrypt the whole data using secret-key encryption algorithms such as DES (Data Encryption Standard) [22]. Secret key encryptions involve large amount of computations.

To achieve adaptability in multimedia data security, security needs in both the application layer and the network layer need to be identified.

## 2.1 Application Layer Multimedia Data Security

Security is an important QoS parameter for applications. For example, different video applications may need different levels of security based on its content. If the video is for military applications, the level of security is high. The additional overhead of applying the most secure cryptographic algorithms is justified. For commercial applications such as pay-per-view video, expensive attacks of the scrambled multimedia data are not interesting to the adversaries because most multimedia videos are not as valuable as military secrets or financial information [14]. The cost to break such encryption code is much higher than the cost to buy the programs. Our research problem is to develop an adaptable scheme to allow different encryption algorithms as discussed in Section 3.1. This research requires experimental studies as discussed in Section 4.1.

## 2.2 Network Layer Multimedia Data Security

In an active network architecture, the network consists of a set of active or non-active nodes. Active nodes run a Node Operating System (NodeOS) and one or more Execution Environments (EEs) that run on the top of NodeOS [1]. Each EE implements a virtual machine which runs the active programs coming with the data packets. The virtual machine can be very general (such as Java Virtual Machine, which is the most popular one) or very specific (such as Spanner [16] in the Smart Packet project, which provide specialized functions for network management tasks).

To achieve different levels of security in network layer, the virtual machine need to provide some primitive operations to perform security-related tasks such as data encryption/decryption, packet authentication, resource reservation, key managements, etc. To understand the design issues of the specialized virtual machine on security-related tasks, we propose the following research questions:

1. Are general script or virtual machines fast enough to implement complicated algorithm such as DES/IDEA or RSA? How fast can mobile code techniques achieve in comparison with the native code implementation?

| Algorithm | Security Ideas | Overhead | Security level |
|---|---|---|---|
| CPA | A secret key is used to change the order of the Huffman codeword list. | low | low |
| VEA | Encryption on sign bits of DCT coefficients of I frame using XOR operation. | low | low |
| MVEA | VEA + encryption on sign bits of motion vectors of P and B frame. | medium | medium |
| RVEA | MVEA with XOR replaced by secret key cryptography. Encrypt only up to 64 bits per macroblock. | high | high |

Table 1: Comparison of three MPEG encryption algorithms

2. What are the most important cryptography algorithm that need to be implemented as common operations in the specialized virtual machine?

3. How big are the active programs when a non-trivial algorithm such as DES/IDEA or RSA decoder is implemented? Is it feasible to implement these algorithms using the mobile codes?

# 3 Related Work

## 3.1 Application Layer Multimedia Data Security

We have developed a series of algorithms for secure MPEG encryption [19, 18, 17, 21, 20]. They are: CPA (Codeword Permutation Algorithm), VEA (Video Encryption Algorithm), MVEA (Modified VEA) and RVEA (Real-time VEA). The basic principles of these algorithms are selective encryption and combining encryption/decryption with MPEG video compression/decompression in one step. These algorithms vary in the cryptographic strength and encrypting/decrypting overhead. Table 1 list the main ideas of the four algorithms and compares the four algorithms in terms of computation overheads and security level each algorithm offers. These algorithms are good candidates for application-level adaptability for security requirements. In addition, these algorithms add a small overhead to the MPEG codec comparing to the approach of encrypting the whole video. Therefore software implementations of these algorithms have been found to meet the real time requirement of MPEG video applications. Our work has been published in a very high quality ACM Multimedia conference [18]. The details of these algorithms can be found in [20].

We found that in typical MPEG videos sign bits occupy less than 10% of a whole video bit stream. Therefore our bit-selection scheme in these encryption algorithms (selecting the sign bits of DCT coefficients and motion vectors) can save 90% of encryption time comparing to algorithms which encrypt the whole video.

We plan to extend the four encryption algorithms to handle the case of multicasting. In a multicasting scenario, the same video need to be sent to receivers with machines of different computing powers. Each receiver can receive a custom-encrypted video with different key and selection of data bits to encrypt. Using different key and encrypting different part of a video will prevent users in a multicasting session from sharing the same video or launching a coordinated attack.

## 3.2 Network Layer Multimedia Data Security

We have designed and implemented an adaptable network architecture, called ADNET [24], which provide mechanisms to allow an application adapt to the resource constraints to achieve improved QoS. Figure 1 shows the architecture of ADNET.

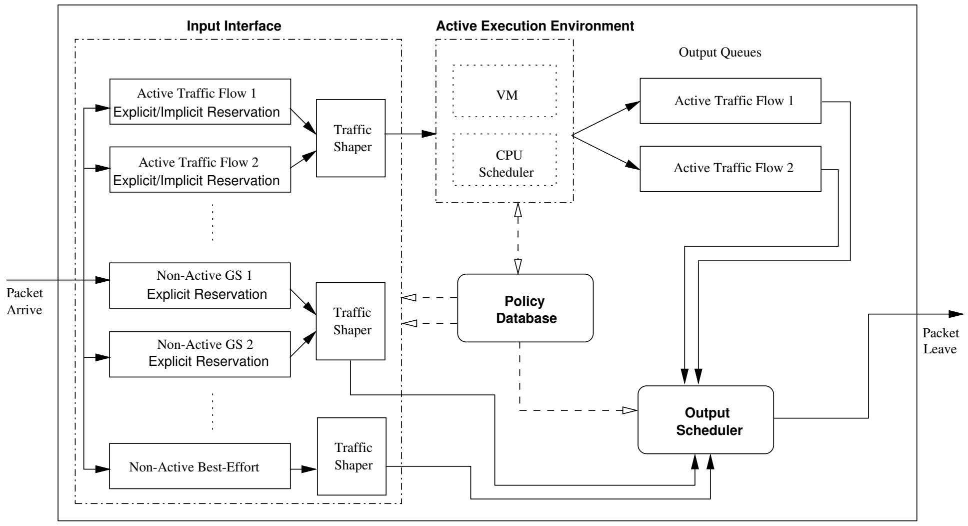


Figure 1: Architecture of an ADNET Router

Adaptable security and safety execution of mobile codes are important features in ADNET. For example, ADNET employs the standardized Secure IP Protocol (IPSEC) [11] to ensure the secure communications. Since the security requirement is an adaptable feature in our design, it can be specified as a QoS parameter when setting up resource reservations. ADNET explicitly includes the resource management module in the design, therefore it can provide true safe execution.

In ADNET, a per-classified-flow state is kept to enforce various policies on the traffic. We argue that per-classified-flow state is a necessity for future networks because it will enhance the security and accountability of future networks.

The virtual machine in ADNET for executing the mobile codes includes a mechanism called *User Installable Operation Codes*. The active program can ask the VM to install part of the codes into a single opcode in either *secure mode* or the *light-weight mode*.

In our experiments with ADNET, we compare three schemes (IP fragmentation, ACTP fragmentation with or without active program) of video transmissions. We find QoS is improved in ACTP scheme with active programs. Our design aims to unify different QoS control mechanisms together to provide a wide range of network services to all users and meet their specific needs. In particular, we will incorporate security-related primitives into our design of the specialized virtual machine in ADNET.

To understand the design issues of the virtual machine in ADNET, we have been conducting experiments to quantify the effectiveness of general capsule programs v.s. specialized processing functions for multimedia data in active routers [25]. The expertise and experiments we obtained in these experiments can be used to conduct more experiments to determine the overheads associated with different security schemes in the active routers.

Another related work is SANE [2]. SANE was designed as a security infrastructure for active networks, and was implemented in the SwitchWare architecture.

# 4 Proposed Solution and Research Tasks

This research is experimental. We have access to multimedia benchmark, software tools to conduct the research (the details are in Section 7).

## 4.1 Experimental Studies in Application Layer Video Security

The resources available to mobile hosts such as CPU power and network bandwidth are very limited. At the same time, mobile users need to have a secure communication channels. Since the security requirements for commercial multimedia applications is not as strict as those for military applications, light-weight encryption algorithms are favored in this case. We have developed a series of light-weight video encryption algorithms [18, 17, 19, 21] which encompass video compression and video encryption in one step. These algorithms vary in computation complexity and encryption strength.

We will identify tuning parameters which can tune the mobile applications to satisfy security requirements under different machine configuration. Specifically, we will investigate and evaluate mechanisms and algorithms that will make the video encryption process adaptable to changing system status such as the power of the machine and/or the load of the system while still maintaining a satisfactory security level. A mobile user can then adapt among those algorithms depending on his need or the status of the system. We plan to answer the following questions through the experimental studies:

- How to maintain satisfactory security levels for video applications in case of system status change?
- What are the guidelines for choosing among different video encryption algorithms?

**Proposed Experiments: Adaptable Bit selection scheme**

- **Purpose:** The purpose of this experiment is to develop adaptable bit selection schemes which are suitable for multicasting for RVEA algorithm. We will study the overhead and analyze the cryptographic strength of the scheme under various configurations. The results of this experiment will be used to guide the design of a mechanism for secure multicasting of video which can provide individualized encryption for each user and prevent the sharing and and coordinated attack of the video session.

- **Method:** We will design new adaptable schemes of selecting bits from MPEG data stream for encryption. The criteria of designing the new schemes are: Low bit extraction overhead, high cryptographic strength, easy to individualize, and adaptable to different computing powers of the receivers. We will implement the new bit-selection schemes under RVEA framework and replace the bit-selection module in RVEA with new schemes. We will measure the CPU time needed in these schemes and compare them with plain MPEG compression algorithms to determine the overheads. We will also perform theoretical and analytical analysis on the new schemes to determine the relative encryption strength of them.

- **Input Parameters:** Different encryption-bit selection algorithms (sign bits of DCT coefficients and motion vectors, etc.), Commercial quality MPEG video traces (video clips JP, LK and TC as described in [23]), number of receivers in the same multicast session.

- **Output Parameters:** We will measure the overhead on CPU time, data compression ratio, and encryption strength under different configuration of the multicast session (number of receivers, computing powers of each receiver, etc.).

- **Analysis and Conclusion to be drawn:** Based on the result from this experiment, We want to design guidelines on the choice of bit-selection schemes under different system configurations. We will obtain the relative encryption strength of these schemes so we can select appropriate level of security to suit the need of different applications. We want to obtain quantitative measures of these schemes under different type of videos so we can provide content-specific tuning of the encryption algorithms. These data can be used to form policies or guidelines which can be used in runtime to adapt among algorithms under different system loads.

## 4.2 Experimental Studies in Network Layer Video Security

Since the questions about security mechanisms in active routers are very general and depend on many different factors such as the choice of virtual machine and encryption algorithm, we plan to investigate one special case which we feel can provide deep insights into the real scenario. Specifically, we will analyze the performance of the MPEG encryption algorithms we have developed in the application layer [18, 17, 19, 21] under C and Java implementations in the active router. Our goal here is to get an estimate of how mobile codes can perform in the problem of secure multimedia data processing because it will be an essential part of our virtual machine.

**Proposed Experiments: Feasibility of mobile codes in network layer video security**

- **Purpose:** The purpose of this experiment is to determine if the current mobile code technologies are fast enough to implement video encryption algorithms. We also want to determine which parts of the MPEG video encryption algorithm consume most of the time and which parts of the algorithm can be extracted and implemented as common operations in the specialized virtual machine.

- **Method:** We will implement the video encryption algorithms in Java language and run the codes on the latest version of Java Virtual Machine. We will compare the encryption and decryption times of both Java and C implementations of the video encryption algorithms. We will run a detail profiling of the Java MPEG encryption algorithms using commercial-quality video clips to determine the relative percentage of running time of each module in MPEG encryption algorithms.

- **Input Parameters:** Different video encryption algorithms (in C and Java implementations), Commercial quality MPEG video traces (video clips JP, LK and TC as described in [23]).

- **Output Parameters:** Overhead on CPU time for encryption/decryption under different implementations, data compression ratio, qualitative encryption strength. Percentage of Running Time for each module in MPEG encryption algorithms.

- **Analysis and Conclusion to be drawn:** We want to quantitatively compare the CPU time requirements for different video encryption algorithms under different implementations. We will develop guidelines of choosing the best encryption algorithm at the most appropriate layer (network layer or application layer) so we can provide different level of security to different applications. The results from this experiments can be used to guide the design of the specialized virtual machine and provide clues of further improvements on the video encryption algorithms.

# 5 Tentative Schedule of Tasks

Development of adaptability features. Architecture design of our integrated application/network secure multimedia processing system (4 months). Implementation of video encryption algorithms and active execution environments (4 months). Experiments, analysis, evaluation, report/papers, and tech transfer (4 months).

# 6 Impact of Proposed Research

This research will lead to algorithms, design principles, prototype systems, experiments with emerging applications such as multimedia and e-commerce. This research provides a foundation for adaptability in the evolution of security features in a distributed systems.

# 7 Infrastructure and Software Tools for Experiments

We are simulating a part of the functionality of ADNET using *ns-2* network simulator. We have extended *ns-2* to includes functionalities described in [24] such as the Active Execution Environment, Input Interface and traffic classification and queue management of the Output

Interface. We are developing a Java MPEG video encryption/decryption system based on the work in [25]. The system will include mobile code modules which perform security-related computations. We have been studying adaptability [8, 9] in distributed systems. We have developed an AVC tool [7] which adds the adaptability to the NV video conferencing tool [10]. It can dynamically adapt to network bandwidth changes while at the same time maintaining reasonable QoS of the video conference session perceived by users. We have built a facility, called active gateway (AG), for experimentation of multimedia communications using Active Networks [13].

# 8 Current Research Activities

We have been actively engaged in developing algorithms and conducting experiments in distributed databases, networks and multimedia computing. This have resulted in several theses, two books, and a series of experimental studies.

- We have developed four MPEG video encryption algorithms [17, 18, 21]. These algorithms can achieve satisfying encryption results with less computations. One important feature of our newly developed MPEG video encryption algorithm, RVEA[21], is its real-time feature. RVEA's bounds its encryption/decryption time to a constant for each video frame.

- Some experiments which compare the execution times of Java and C implementations of MPEG decoding algorithms have already been performed in our lab. We plan to extend this further by using the existing experiment environments to study the strength and the efficiency of different security algorithm which will be built into the virtual machine.

# 9 Plans for Continuation of Research/Tech Transfer

- We have been working closely with representative from CISCO (W. Brian Beal) on the work of security in transmission of multimedia to implement some ideas and algorithms we have developed and published.

- Informix Corporation is interested in security transmission of multimedia data. We are exploring the possibility of sharing results of our experiments on "Experimental Evaluation of Design Tradeoff in Specialized Virtual Machine for Multimedia Traffic in Active Networks" with Informix Corporation (Shalab Goel and Suresh Yanamadala).

- Army Research Lab and AT&T Corporation are also interested in corporating with us on this research.

- Dr. Sheng-Yih Wang has given a presentation of the work at Foundry Networks and Informix Corporation.

# Biographical Sketch

**BHARAT BHARGAVA**
**Computer Science Department**
**Purdue University**
**bb@cs.purdue.edu**

## Education

| | | |
|---|---|---|
| 1974 | Ph.D., Electrical Engineering | Purdue University |

## Professional Experience

| | |
|---|---|
| 1973-1976 | Research Associate (Regenstrief Institute), Department of Medicine, Indiana University |
| 1978-Summer | Visiting Faculty, Stanford University |
| 1976-1978 | Assistant Professor, Cleveland State University |
| 1978-1984 | Assistant Professor, University of Pittsburgh |
| 1984- | Professor, Purdue University |

## Honors and Awards

- Best Research Paper Award, IEEE Data Engineering Conference, 1988
- Fellow of Institute of Electrical and Electronics Engineers (IEEE)
- Meritorious Service Certificate from IEEE Computer Society
- Fellow of Institution of Electronics and Telecommunications Engineers (IETE)
- Second Best Paper, IEEE Distributed Computing Systems Conference, 1995
- Outstanding Instructor Award (ACM student chapter), 1996
- Golden Core Member of IEEE Computer Society
- Technical Achievement Award, IEEE Computer Society, 2000

## Editorial Boards

1. Editor of International Journal of Multi-Media Systems
2. Editor of International Journal of Cooperative Information Systems

## Current Students

Ahsan Habib, Santosh Krishna, Binita, David McClure and Sarat Babu Kamisetty.

# Research Associate

**SHENG-YIH WANG**
**Computer Science Department**
**Purdue University**
**swang@cs.purdue.edu**

## Education

| | | |
|---|---|---|
| 2000 | Ph.D. Computer Science | Purdue University, West Lafayette, Indiana |
| 1991 | M.S. Computer Science | National Tsing-Hua University, Taiwan |
| 1989 | B.S. Mathematics | National Taiwan University, Taiwan |

## Professional Experience

February, 2000 Research Associate, Department of Computer Science, Purdue University, West Lafayette, IN 47907

## Selected Publications

- Sheng-Yih Wang. "Approaches to Multimedia Traffic Management and Control", *Ph.D. thesis, Department of Computer Science, Purdue University*, May 2000.
- Sheng-Yih Wang and Bharat Bhargava. "Experimental Evaluation of Design Tradeoff in Specialized Virtual Machine for Multimedia Traffic in Active Networks". To appear in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2000)*, July 30 - August 2, 2000.
- Sheng-Yih Wang and Bharat Bhargava. "An Adaptable Network Architecture for Multimedia Traffic Management and Control". To appear in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2000)*, July 30 - August 2, 2000.
- Changgui Shi, Sheng-Yih Wang and Bharat Bhargava. "MPEG Video Encryption in Real-Time Using Secret Key Cryptography", in *Proceedings of the 1999 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA '99)*, June 1999.
- Sheng-Yih Wang and Bharat Bhargava, "A Fragmentation Scheme for Multimedia Traffics in Active Networks", in *Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems (SRDS'98)*, October 1998.
- Sheng-Yih Wang and Bharat Bhargava, "Multi-pass Transmission Policy: An Effective Method of Transmitting Large Multimedia Objects in the Wide-Area Network", in *Proceedings of IEEE COMPSAC'97*, Washington, D.C., August, 1997.

# References


[1] Active Network Working Group (K. L. Calvert, ed.). Architectural Framework for Active Networks Version 1.0. URL `http://www.dcs.uky.edu/~calvert/arch-1-0.ps`, July 1999.

[2] D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, Steve Muir, and Jonathan M. Smith. Secure Quality of Service Handling: SQoSH. *IEEE Communication Magazine*, 38(4), April 2000.

[3] Elan Amir, Steven McCanne, and Randy H. Katz. An Active Service Framework and its Application to Real-time Multimedia Transcoding. In *Proceedings of the ACM SIGCOMM*, Vancouver, British Columbia, Canada, September 1998.

[4] B. Bhargava. Experiments in Adaptability in Multimedia Systems. In *Lecture Notes in Computer Science, 10th International Conference and Workshop on Database and Expert Systems (DEXA'99)*, Florence, Italy, 1999.

[5] Bharat Bhargava. Guest Editorial: Digital Libraries and Multimedia. *Multimedia Tools and Applications*, 10(2/3), April 2000.

[6] Bharat Bhargava and Melliyal Annamalai. A Communication Framework for Digital Libraries. *Multimedia Tools and Applications*, 10(2/3), April 2000.

[7] Bharat Bhargava, Shunge Li, Shalab Goel, Chunying Xie, and Changsheng Xu. Performance studies for an adaptive video-conferencing system. In *Proceedings of the International Conference on Multimedia Information Systems (MULTIMEDIA 96), New Delhi, India*, pages 106–116. IETE, McGRAW HILL, February 1996.

[8] Bharat Bhargava and John Riedl. A Model for Adaptable Systems for Transaction Processing. *IEEE Transactions on Knowledge and Data Engineering*, 1(4), December 1989.

[9] Bharat Bhargava and John Riedl. The Raid Distributed Database System. *IEEE Transaction on Software Engineering*, 15(6), June 1989.

[10] Ron Frederick. Experiences with Real-Time Software Video Compression. In *Proceedings of the Packet Video Workshop*, Portland, Oregon, September 1994.

[11] Stephen Kent and Randall Atkinson. Security Architecture for the Internet Protocol. *RFC 2401*, November 1998.

[12] Shunge Li. *Quality of Service Control for Distributed Multimedia Systems*. PhD thesis, Department of Computer Science, Purdue University, December 1997.

[13] Shunge Li and Bharat Bhargava. Active Gateway: A Facility for Video Conferencing Traffic Control. In *Proceedings of COMPSAC'97, Washington, D.C.*, pages 308–311. IEEE, August 1997.

[14] B. Macq and J. Quisquater. Cryptoloy for Digital TV Broadcasting. *Proceedings of the IEEE, Vol. 83(6):944-957*, June 1995.

[15] Gary McGraw and Edward Felten. *Java Security: Hostile Applets, Holes and Antidotes.* John Wiley & Sons, 1997.

[16] B. Schwartz, A. Jackson, T. Strayer, W. Zhou, R. Rockwell, and C. Partridge. Smart Packets for Active Networks. In *Proceedings of the Second IEEE Conference on Open Architectur es and Network Programming*, New York City, New York, March 1999.

[17] C. Shi and B. Bhargava. An Efficient MPEG Video Encryption Algorithm. *In Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems, pp. 381-386*, Oct. 1998.

[18] C. Shi and B. Bhargava. A Fast MPEG Video Encryption Algorithm. *In Proceedings of the 6th ACM International Multimedia Conference, Bristol, UK*, pages 81–88, September 1998.

[19] C. Shi and B. Bhargava. Light-weight MPEG Video Encryption Algorithm. In *Proc. of the Int'l Conf. on Multimedia(Multimedia98, Shaping the Future), January 23 – 25, pages 55–61, New Delhi, India.* IETE, Tata Mcgraw-Hill Publishing Company, 1998.

[20] C. Shi, S. Wang, and B. Bhargava. MPEG Video Encryption Algorithms. *Submitted for journal publication*, August 1999.

[21] C. Shi, S. Wang, and B. Bhargava. MPEG Video Encryption in Real-time Using Secret Key Cryptography. In *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'99)*, Las Vegas, Nevada, June 1999.

[22] Douglas R. Stinson. *Cryptography Theory and Practice.* CRC Press, Inc., New York, 1995.

[23] S. Wang and B. Bhargava. An Adaptable Network Architecture for Multimedia Traffic Management and Control. Technical Report CSD-99-048, Purdue University, Department of Computer Sciences, November 1999.

[24] S. Wang and B. Bhargava. An Adaptable Network Architecture for Multimedia Traffic Management and Control. In *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2000)*, New York, NY, July 2000.

[25] S. Wang and B. Bhargava. Experimental Evaluation of Design Tradeoff in Specialized Virtual Machine for Multimedia Traffic in Active Networks. In *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2000)*, New York, NY, July 2000.