A Security Protocol for Real Time Applications (RTA)

M. Anand Kumar and Dr. S. Karthikeyan

Abstract—Real time applications are growing rapidly in the recent past. In the recent times many business organizations have been deploying Real Time Applications over the internet like Video Conferencing, VOIP and other Multimedia services.These applications are used by thousand of users and controlled by different administrative entities The need to protect user's data and infrastructures becomes more important than ever. Cryptography is used to provide the security needed for real time applications. Since Real time applications contain confidential data, Current encryption techniques are not appropriate, because most of RTA is served via Internet; there is a need of strong security mechanism. In this paper a new security protocol called Real time security protocol (RTSP) is proposed. Experimental results show that the proposed model provides better security with minimum overhead in terms of processing

Key words Cryptography, Real Time applications, Encryption and security

I Introduction

Real time applications play a vital role in the current technology world. There are several Organizations, business, workgroups, research bodies, institutions and researchers are using the real time applications such as video conference applications, VOIP, online gaming, community storage solutions, e-commerce transactions, chatting and instant messaging. With the rapid growth of internet and its applications, there is great demand for Network security [1].

Network security is mainly concerned with protecting sensitive data from unauthorized users and applications. But in the current scenario securing data is often approached from different viewpoint. With the increasing use of Internet for business applications, there is a great demand for Quality of service for real time applications. The application that is increasing day-by-day needs a consistent control protocols for providing quality of service (QOS). Because of these reasons the need for security in the Internet is stronger than ever [2].

The rest of the paper is organized as follows. Cryptography algorithms are described in section II that is followed by problem description in section III. The proposed architecture is presented in section IV and the performance is evaluated in the section V. Finally we conclude in section VI

II Cryptography Algorithms

Cryptography is a process, which ena bles user to maintain privacy of data they send to each other even in the presence of an adversary with access to the communication Channel [3]. It is a science that uses mathematical calculations to encrypt and decrypt data. It also permits the users to store sensitive information or transmit it across insecure networks. So that it cannot be read by anyone except the intended recipient. While providing privacy remains a central goal, the field has expanded to encompass many others including not just other goals of communication security such as guaranteeing integrity and authenticity of communications but also many more sophisticated and fascinating goals. Basically two types of cryptographic algorithms exist such as symmetric and asymmetric algorithms. Some of the symmetric algorithms are DES, AES, CAST – 128/256, International Data Encryption algorithm (IDEA), Rivest Ciphers (RC1 – RC6), Blowfish, Two fish, Camellia, Secure and fast encryption routine (SAFER), and SEED. Some of the asymmetric algorithms are RSA, Diffie- Hellman, Digital Signature Algorithm (DSA), Elgamal, Elliptic Curve Cryptography (ECC), Public-Key Cryptography Standards (PKCS), Cramer-Shoup, Key Exchange Algorithm (KEA), and LUC. These algorithms are analyzed to use them in the proposed architecture. From the analysis it shows that Blowfish that is a symmetric cryptography is highly secure with good performance when compared to others. In this proposed architecture Blowfish algorithm is used along with elgamal and SHA hash algorithm [5].

A. Blowfish.

Blowfish: Blowfish [4] is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, a key and data-dependent substitution. All operations are EX-ORs and additions on 32-bit words Blowfish is successor to two fish

B. Elgamal Algorithm

It is a public-private encryption algorithm [5] [11] where each user has a public key and a corresponding private key. The public key can be used to encrypt data, but private key is used to decrypt the data. If sender publish his public key then everyone can encrypt a message using sender's public key, but only the sender can decrypt the message. Elgamal is based on the Diffie Hellman key agreement. Elgamal algorithm is analyzed in many environments. The analysis shows the strong nature of the algorithm. It is very difficult to break the key or data. Elgamal encryption is implemented by using three components namely the key generator, the encryption algorithm and the decryption algorithm.

C. SHA -2 Hashing

In recent years the most widely used hash function has been the secure hash algorithm. The SHA1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA1 is a technical revision of SHA (FIPS 180). A circular left shift operation has been added to the SHA (FIPS 180). SHA1 improves the security provided by the SHA standard. The SHA1 is based on principles similar to those used by the MD4 message digest algorithm.

III Problem Description

The Internet has worked so far with a best effort traffic model, every packet is treated (forwarded or discarded) equally. This is a very simple and efficient model. Recently many interactive or real-time services have been introduced and the economical importance of the Internet has grown. The IP phones and services based on that technology is threatening the traditional circuit-switched telephone services, especially on long-distance services. Transmitting interactive real-time media is the greatest challenge in packet based networks. The end-to-end delay, the delay variations (jitter), and the packet loss must not exceed some time limits; otherwise, usability of the service degrades badly. Many companies have been deploying RTA over the internet like VoIP, Video

Conferencing and other Multimedia services in recent years. The need to protect users, data and infrastructures becomes more crucial than ever. Encryption is used to provide the security needed for RTA. Since RTA contains more confidential data, the existing encryption techniques are not appropriate, because most of RTA is implemented on the Internet, the encryption and decryption techniques should be more secure than any other applications. Another important aspect of the RTA is time delay. The encryption and decryption technique has to take minimal time to achieve acceptable end-to-end delays. This aspect is beyond the scope of this paper. Here we propose a new algorithm called Real Time Security Protocol (RTSP) to provide the better security than existing security algorithms.

Iv. Proposed System

The proposed system contains a new security algorithm called Real Time Security protocol (RTSP). It was designed in such a way that it provides very high security for Real time applications Cryptographic algorithms are included in the proposed protocol

Sender Side Algorithm

1. The data is encrypted using BLF Ct = BLF (Pt)
2. The keyk is Encrypted using ELG Ck= ELG (k)
3. Message digest for data using SHA dg = SHA (Pt)
4. Encrypt digest using ELG Cm= ELG (dg)
5. Send Ct, Ck, Cm to destination

Receiver Side Algorithm

1. The key is decrypted using ELG Dk = ELG (k) = k
2. The key k is used to decrypt text Dt=ID (Ct)= Pt
3. Message digest for data using SHA MD = SHA (Pt) = dg
4. Decrypt digest using ELG Pm = ELG (Cm) = dg
5. Compare dg from Step 3 and Step 4.
6. If equal data is accepted else rejected.

Where BLF = Blowfish algorithm Pt = Plain text

ELG = Elgamal algorithm, Ck = Cipher Key, Ct = Cipher text, dg = Message Digest

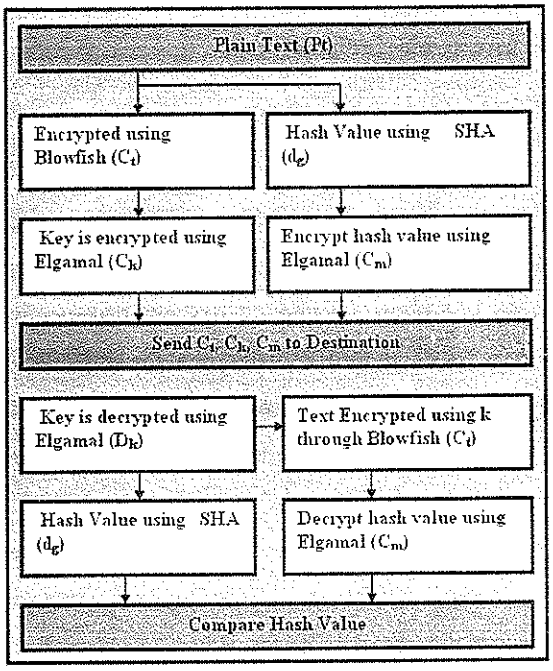
Plain Text (Pt)
Encrypted using Blowfish (C_t)
Hash Value using SHA (d_g)
Key is encrypted using Elgamal (C_k)
Encrypt hash value using Elgamal (C_m)
Send C_t, C_k, C_m to Destination
Key is decrypted using Elgamal (D_k)
Text Encrypted using k through Blowfish (C_t)
Hash Value using SHA (d_g)
Decrypt hash value using Elgamal (C_m)
Compare Hash Value

Figure 1 : RTSP Security Architecture

In the proposed architecture three cryptography algorithms are used to provide the security. First the plain text P_t is encrypted using Blowfish encryption. The key_k that is used for encryption is further encrypted using Elgamal encryption. Then the cipher text C_t along with the cipher key C_k will be sent to destination. At the same time message digest for the plain text will be calculated using SHA. Then the message digest will be encrypted using Elgamal encryption. Now Cm will be sent to destination along with C_t, C_k. At the receiver end first the key is decrypted using elgamal decryption. Next with the obtained key the Cipher text is decrypted. At the same time message digest is calculated using SHA. Then the message digest that is received from the source end is compared with the digest that is calculated in the receiver side. The RTSP architecture that is proposed here uses both symmetric and asymmetric cryptography to provide all the aspect of network security such as Confidentiality, integrity, authentication, non-repudiation, availability and access control. The algorithm that is described above provides a good security under any environment and can be used as add- ins like IPsec.

V Performance Evaluation

In the previous work [7] different set of algorithms were used such as IDEA, Elgamal and MD5. The result [7] shows that the performance is very low when compared to the original architecture. It also shows that encryption time is very high for IDEA algorithm for large file. It is proved that if there is decrease in encryption time then the performance can be increased. In order to improve the performance, Blowfish is used in place of IDEA and SHA -512 is used in the place of MD5. To demonstrate the performance for the proposed architecture, a series of simulation runs are performed on a variety of set of data. The proposed algorithm is compared with AES algorithm to evaluate the performance and the security. The algorithm is executed as five rounds each with different number of files. Several performance metrics are used such as encryption time, Decryption time, CPU process time, CPU clock cycles and battery power. The encryption time was calculated using the above mentioned metrics. Encryption time is the total time taken to produce a cipher text from plain text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption. The throughput of the encryption scheme is calculated as the total encrypted plaintext in bytes divided by the encryption time. Decryption time is the total time taken to produce the plain text from plain text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption. The throughput of the decryption scheme is calculated as the total decrypted plaintext in bytes divided by the decryption time. The CPU process time is the time that is required to a CPU is dedicated only to the particular process of calculations. It reflects the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy. Table 1 provides the encryption time for the proposed protocol and Table 2 provides the decryption time for the proposed protocol.

TABLE I
ENCRYPTION TIME (MILLISECONDS)

Round	No of Files	AES algorithm	Proposed algorithm
1	1	241 ms	287 ms
2	3	736 ms	790 ms
3	5	1202 ms	1290 ms
4	8	851 ms	911 ms
5	10	2102 ms	2210 ms

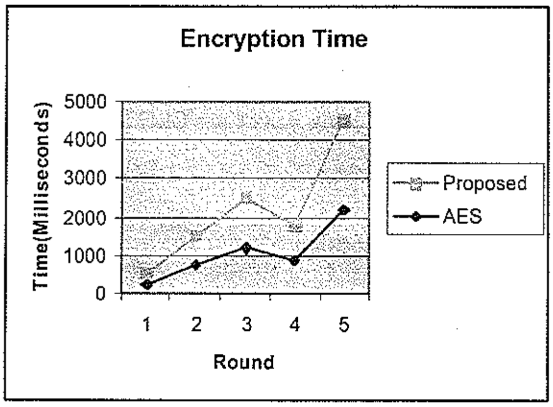

Figure 2 : Encryption time analysis

TABLE 2
DECRYPTION TIME (MILLISECONDS)

Round	No of Files	AES algorithm	Proposed algorithm
1	1	250 ms	290 ms
2	3	750 ms	792 ms
3	5	1200 ms	1321 ms
4	8	865 ms	921 ms
5	10	2200 ms	2321 ms

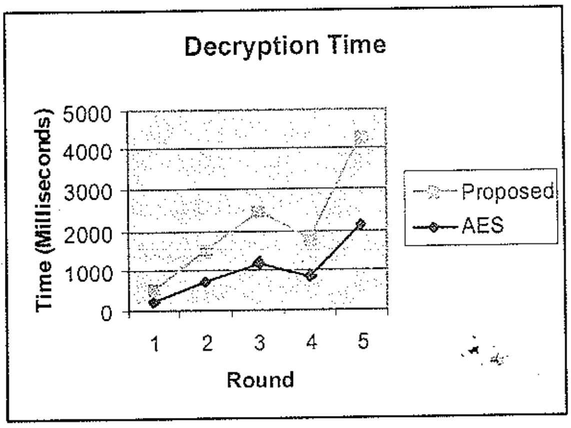

Figure 3 : Decryption time analysis

From the analysis, it shows that the proposed architecture has slightly low performance when compared to that of existing AES algorithm. But in the case of security aspects, the proposed algorithm is better to provide the sophisticated security when compare to the existing algorithm. It is also identified that blowfish algorithm used in the proposed architecture takes more time to encrypt the data. It is also identified that if there is a decrease in the encryption time then the performance will be increased. Cryptanalysis is carried out in the encrypted file. It was found that the encrypted file with this algorithm is difficult to break.

VI Conclusion And Future Work

This paper has outlined the need for security for the real time applications. It also outlines new ideas to design efficient security mechanism for the RTA applications. With minor changes in the existing model, high level of security can be obtained. Some of the potential applications such as video conference applications, VOIP, online gaming, community storage solutions, e-commerce transactions, chatting and instant messaging can be secured using this proposed algorithm.. It is also identified that a single algorithm with all the security provision is required to provide better security with good performance. Based on this work, we have planned to implement a new 512-bit block cipher which can be used specifically for real time applications.

References

[1] Ahmed h. Omari and basil m. Al-kasasbeh, "A New Cryptographic Algorithm for the Real Time Applications 'Proceedings of the 7th WSEAS International Conference on Information Security and Privacy, 2008

[2] E. Cole, R. Krutz and J. W. Conley, Network Security Bible, Wiley Publishing Inc, 2005.

[3] Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E," Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect", International Journal of Computer Science and Network Security, 8(3), 2008

[4] Tingyuan Nie Teng Zhang," A study of DES and Blowfish encryption algorithm, Tencon IEEE Conference,, 2009

[5] Douligeris.C, Douligeris, C, Serpanos, D. Serpanos, D," IP Security (IPSec)", IEEE Book: Network Security: Current Status and Future Directions, 65 – 82, 2007

[6] Dewu Xu Wei Chen, "3G communication encryption algorithm based on ECC-ElGamal",

2nd International conference on signal processing systems,Vol :3, 2010

[7] Anand Kumar. M, Dr. S. Karthikeyan, "A New security architecture for TCP/IP Protocol suite", International Journal of Advanced Research in Computer Science", 1(3), 177-181.

[8] Hiromi, R.; Yoshifuji, H., "Problems on IPv4-IPv6 network transition," Proceedings of the internationalSymposium on Applications and the Internet Workshop, Saint 2005

[9] Heng Yin Haining Wang."Building an Application-Aware IPsec Policy System", IEEE/ ACM Transactions on Networking 15(6), 1502 – 1513, 2007.

[10] L.Colitti, G. D. Battista, and M. Patrignani," IPv6-in-IPv4 tunnel discovery: methods and experimental results", IEEE Transactions on Network and Service Management, vol. 1, no.1, 2004.

[11] Mohammad Al-Jarrah, Abdel-Karim R. Tamimi,"A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancemen",. IEEE Conference in Innovations in Information Technology,1-5, 2007.

[12] J. Dray, NIST Performance Analysis of the Field Round Java AES Candidates, online: http:// csrc.nist.gov/encryption/aes/roubd2/conf2/papers/ 8-jdray.pdf, 2000, accessed on Sept. 1, 2008.

[13] R. Chandramouli, Battery power-aware encryption," ACM Transactions on Information and Sys- tem Security (TISSEC), vol. 9, no. 2, pp. 162-180, May 2006.

[14] M. H. Ibrahim, Receiver-deniable public-key en- cryption," International Journal of Network Secu rity, vol. 8, no. 2, pp. 159-165, 2009.

[15] A. Nadeem, A performance comparison of data encryption algorithms," IEEE Information and Com- munication Technologies, pp. 84-89, 2006.

[16] Results of Comparing Tens of Encryption Algorithms Using Di®erent Settings- Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http:// www.eskimo.com/ weidai/benchmarks.html)

Author's Biography

M. Anand Kumar has completed M.Sc and M.Phil in computer science and currently working as a Lecturer in karpagam University having six years experience in teaching. He is pursuing PhD in computer Science under the guidance of Dr. S. Karthikeyan, who is Working as Asst. Professor in department of Information Technology College of Applied Sciences Sultanate of Oman. His area of research includes network security and information security. He has presented fifteen papers in national conferences and four papers in international conferences. He has published six papers in international journals

Dr.S.Karthikeyan presently working as Assistant Professor, College of Applied Sciences, Oman and previously he was a Senior Lecturer at Caledonian College of Engineering, Oman. He was a Professor & Director at Karpagam University, School of Computer Science and Applications, Coimbatore. He has total of 14 years of teaching and research experience. Dr.Karthikeyan completed his PhD at Alagappa University, Karaikudi, India in the area of Network Security, Computer Science and Engineering by Feb 2008. He has 32 research papers and guiding 11 PhD research scholars from various universities in India and he has also guided 19 M.Phil students. He is Chief and guest editor of various national and international journals. He has chaired many conference sessions and served as Technical Committee member of various boards at various colleges, universities and conferences.