Survey on Secure Transmission Scheme for Cryptography with Least Overhead

Pallavi M O
Ait Tumkur
Karnataka India,

Prof. Shivamurthy
Ait Tumkur
Karnataka India,

***Abstract*— To fulfill the needs for secure and lightweight data transmission approach, we propose a new plain text transmission Technique, which uses compressed bit stream of information as a mean of communications. This technique reduces channel overhead, information loss, and high bandwidth requirement. It capitalizes on the data security as it nullifies information notching, and prevents the attempt of modification by unauthorized third party. The proposed scheme expands security by incorporating pattern recognition, data encryption using SDES encryption technique, and reduces extra overhead by data density technique. To justify the efficiency of our proposed technique, we tested our proposed technique with different input text sizes. The security part, related with the proposed technique is tested by means of preventing capacity against the different security attacks. The efficiency of the proposed security part is measured by calculating the in sequence loss during the transmission. The proposed density technique is tested by taking standard Calgary Corpus as inputs.**

***Keywords*— Bit stream; channel overhead; high band width; information notching; pattern recognition;**

I. INTRODUCTION

The art of protecting information by transforming, it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The word is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

II. PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came

soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

III. BITSTREAM

A byte stream is a series of bytes. Typically these are values from a range of 256 distinct values (octets), and so the term octet stream is sometimes used to refer to the same thing. An octet may be encoded as a sequence of 8 bits in multiple different ways (see bendiness) so there is no unique and direct translation between byte streams and bit streams. In practice, bit streams are not used directly to encode byte streams; a communication channel may use a signaling method that does not directly translate to bits (for instance, by transmitting signals of multiple frequencies) and typically also encodes other information such as framing and error correction together with its data.

Bit streams and byte streams are used extensively in telecommunications and computing: for example, the SDH communications technology transports synchronous bit streams, and the TCP communications protocol transports a byte stream without synchronous timing.

IV. HIGH BANDWIDTH DIGITAL CONTENT PROTOCOL

High-bandwidth Digital Content Protection (HDCP) is a form of digital copy protection developed by Intel Corporation to prevent copying of digital audio and video content as it travels across connections. Types of connections include Display Port (DP), Digital Visual Interface (DVI), and High-Definition Multimedia Interface (HDMI), as well as less popular, or now defunct, protocols like Gigabit Video Interface (GVIF) and Unified Display Interface (UDI).

The system is meant to stop HDCP-encrypted content from being played on unauthorized devices or devices which have been modified to copy HDCP content before sending data, a transmitting device checks that the receiver is authorized to receive it. If so, the transmitter encrypts the data to prevent eavesdropping as it flows to the receiver.

In order to make a device that plays material protected by HDCP, the manufacturer must obtain a license from Intel subsidiary Digital Content Protection LLC, pay an annual fee, and submit to various conditions. For example, the device cannot be designed to copy; it must "frustrate attempts to defeat the content protection requirements";it must not transmit high definition protected video to non-HDCP receivers; and DVD-Audio material can be played only at CD-audio quality by non-HDCP digital audio outputs (analog audio outputs have no quality limits).

Cryptanalysis researchers demonstrated flaws in HDCP as early as 2001. In September 2010, an HDCP master key that allows for the generation of valid device keys—rendering the key revocation feature of HDCP useless—was released to the public. Intel has confirmed that the crack is real, and believes the master key was reverse engineered rather than leaked. In practical terms, the impact of the crack has been described as "the digital equivalent of pointing a video camera at the TV", and of limited importance for copyright infringers because the encryption of high-definition discs has been attacked directly, without the loss of interactive features like menus. Intel threatened to sue anyone producing an unlicensed device.

V. PRIOR STUDY WORK

Zhang et al. [1] studied this practical problem and propose a Rate-Distortion-Authentication (R-D-A) optimized streaming technique for authenticated video. Based on packets' importance in terms of both video quality and authentication dependencies, the proposed technique computes a packet transmission schedule that minimizes the expected end-to-end distortion of the authenticated video at the receiver subject to a constraint on the average transmission rate. Simulation results based on H.264 JM 10.2 and NS-2 demonstrate that their proposed R-D-A optimized streaming technique substantially outperforms both prior (authentication-unaware) R-D optimized streaming techniques and data stream authentication techniques. In particular, when the channel capacity is below the source rate, the PSNR of authenticated video quickly drops to unacceptable levels using conventional R-D optimized streaming techniques, while the proposed R-D-A

Optimization technique still maintains optimized video quality. Furthermore, they examine a low-complexity version of the proposed algorithm, and also an enhanced version which accounts for the multiple deadlines associated with each packet, which is introduced by stream authentication.

Rinza et al. [2] decrypted the information using probability leads to a more thorough job, because you have to know the percent- age of each of the letters of the language that is being analyzed here is Spanish. You can consider not only the probabilities of the letters also syllables, set of three, four letters and even words. Then you have this thing to do is make comparisons of the frequencies of cipher text and the frequencies of the language to begin to replace by a correspondence.

MSVS et al. [3] presented an attempt is made to analyze the text based crypto model using frequency distribution of character code points as a parameter with specific study on Indic scripts. The encryption and decryption process is tested in comparison with English and also on Telugu with different key sizes. Evaluation of the model is carried out with the help of frequency distribution as one of the prominent characteristic of text. Crypto analysis is carried out on both the languages with 8-bit key and the percentage of matches in the reverse transformation is presented. The mapping for English text ranges from 23 % to 50 % where as for Telugu it ranges from 10% to 20%. The analysis is extended to 16-bit key size on Telugu text. The mapping for 16-bit is observed in the range of 1% to 10%. If the text complexities are considered for each script, greater levels of security are observed with smaller key sizes. Evaluation of the proposed model on other Indic scripts of the same nature is in progress. The proposed cryptographic model is implemented now by considering 16-bit key on Telugu using the above mentioned approach. Mapping is carried out between the characters of plain text and cipher text based on these frequencies. The results indicate that the percentage of retrieved plain text is varying between 10- 20% whereas for 16-bit key the observed results are found in the range 1-10% only.

Vimalathithan and Valarmathi [4] have presented an algorithm for the cryptanalysis of Simplified Data Encryption Standard is presented. The time complexity of the proposed approach has been reduced drastically when compared to the Brute-Force attack. Though SDES is a simple encryption algorithm, this is a promising method and can be adopted to handle other complex block ciphers like DES and AES. The cost function used here can be applied for other block ciphers also. The future works are extending this approach for attacking DES and AES ciphers.

Vimalathithan and Valarmathi [5] presented a novel approach Genetic Swarm optimization algorithm for the cryptanalysis of Data Encryption Standard to breaks the key successfully. The fitness function used here is not restricted and can be applied for other block ciphers also. The fitness function used here can be used only for known plain text attack and cannot be applied for Cipher text only attack. The future work is to create a better fitness function and to apply GSO for attacking cipher text only for DES..

Saveetha et al. [6] have proposed tabu search in 1983 to allow local search methods to overcome local optima. Tabu search is to perform local search in local optimum by allowing non-improving moves. They maintain a list called tabu list to record the recent history of the search. It is also one of the optimization heuristics techniques which prevent the search from returning to a previously explored region of the solution space immediately. Hence it maintains a list of previous solutions, which are called “tabu‟; hence the name of the technique. Performance of the algorithm depends on the size of the tabu list. In the tabu list two randomly chosen key elements are swapped to generate candidate solutions. In each iteration one worst solution in the tabu list will be eliminated with newer one.

Jhajharia et al. [7] illustrated an algorithm for Public Key Cryptography (PKC) using the hybrid concept of two evolutionary algorithms, Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) respectively. PSO alone are fast and easy to implement, they follow the procedures of common evolutionary algorithm and posses memory feature which is absent in GA making it more valuable. In GA whole population or set of individual chromosome work together sharing information to reach an optimal solution whereas PSO focuses on only the best possible solution. Particles in PSO converge in small optimal area quickly. PSO uses a set of fine fit initial keys as input from key domain generated by GA and outputs the position of key having the highest fitness among the keys. Thus, PSO-GA algorithm aims here for generating the fittest among the fine fit keys in key domain containing best keys of highest possible strength. The results produced by this hybrid algorithm to be tested for frequency test, gap test, auto-correlation test, binary derivative test, change point test, serial test, run test and also to check for the linear complexity of key proving its validity and practical use of the proposed work in PKC.

Nalini et al. [8] established the applicability of a couple of optimization heuristics to crypt-analysis studies; one based on thermo statistical persistency applied to simulated annealing and the other one based on particle swarm principle. Though both methods lead to successful attacks, their improvised version of group swarm optimization yields better performance. As a vehicle of demonstration of their concept, they choose simple yet representative block ciphers such as computationally tractable versions of DES, for their studies. They also propose an extension to this concept by introducing a unique concept of group of swarms. This technique when applied to cryptanalysis of their candidate block cipher has yielded better performance compared to the simulated annealing algorithm implemented with thermo statistical persistency principle incorporated into it.

Selcuk [9] presented an analytical calculation of the success probability of linear and differential cryptanalytic attacks. The results apply to an extended sense of the term \success" where the correct key is found not necessarily as the highest-ranking candidate but within a set of high-ranking candidates. Experimental results show that the analysis provides accurate results in most cases, especially in linear cryptanalysis. In cases where the results are less accurate, as in certain cases of differential cryptanalysis, the results are useful to provide approximate estimates of the success probability and the necessary plaintext requirement. The

analysis also reveals that the attacked key length in differential cryptanalysis is one of the factors that affect the success probability directly besides the signal to noise ratio and the available plaintext amount.

Laskari et al. [10] illustrated a brief review to cryptography and a CI method is initially provided. Then, a short survey of the applications of CI to cryptographic problems follows, and their contribution in this field is analytically presented. More specifically, at first three cryptographic problems derived from classical public key cryptosystems are formulated as discrete optimization tasks and Evolutionary Computation (EC) methods are applied to address them. Next, EC methods for the partial cryptanalysis of a Feistel cipher, the Data Encryption Standard reduced to four and six rounds, respectively, are considered.

VI. CONCLUSION

One of the biggest and fastest growing applications of cryptography today, though, is electronic commerce (e-commerce), a term that itself begs for a formal definition.

REFERENCES

[1] Z. Zhang; S. Qibin; W. Wai-Choong; J. Apostolopoulos; S. Wee, "Rate-Distortion-Authentication Optimized Streaming of Authenticated Video," Circuits and Systems for Video Technology, IEEE Transactions on , vol.17, no.5, pp.544-557, May 2007

[2] Rinza, B., Fernando Zacarias Flores, Luna Pérez Mauricio, and M. C. Antonio. "Decryption through the likelihood of frequency of letters." Benemerita Universidad Autonoma de Puebla.

[3] Bhadri Raju MSVS1, Vishnu Vardhan B2, Naidu G A3, Pratap Reddy L4, and Vinaya Babu, “Effect of Language Complexity on Deciphering Substitution Ciphers - A Case Study on Telugu” , International Journal of Security and Its Applications Vol. 4, No. 1, January, 2010

[4] Vimalathithan.R1, Dr.M.L.Valarmathi, “Cryptanalysis of S-DES using Genetic Algorithm”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009

[5] Vimalathithan. R, M. L. Valarmathi, “Cryptanalysis of DES using Computational Intelligence”, Journal of Scientific Research, Vol. 55, No. 2, pp. 237-244, 2011

[6] P. Saveetha, S. Arumugam, K. Kiruthikadevi, “ Cryptography and the Optimization Heuristics Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue. 10, October 2014

[7] Smita Jhajharia, Swati Mishra, Siddharth Bali, “ Public Key Cryptography Using Particle Swarm Optimization and Genetic Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013

[8] Nalini N and G. Raghavendra Rao, “Cryptanalysis of Block Ciphers via Improvised Particle Swarm Optimization and Extended Simulated Annealing Techniques”, International Journal of Network Security, Vol.6, No.3, PP.342–353, 2008

[9] Selçuk, Ali Aydın. "On probability of success in linear and differential cryptanalysis." Journal of Cryptology 21, no. 1, pp.131-147, 2008

[10] Laskari, Elena C., Gerasimos C. Meletiou, Yannis C. Stamatiou, and Michael N. Vrahatis. "Cryptography and Cryptanalysis Through Computational Intelligence." In Computational Intelligence in Information Assurance and Security, pp. 1-49. Springer Berlin Heidelberg, 2007.