TCP AND UDP-BASED SECURE MESSAGE TRANSMISSION TO TARGET DEVICES

A·Durga Pavani[1,] Mr.A. Mallesh[2]

[1] Assoc. Professor, Department of Computer Applications, Aurora's PG College (MBA), Uppal, Hyderabad

Email: pavanidurga@gmail.com

[2]Assistant Professor, Department of Computer Applications, Aurora's PG College (MBA), Uppal, Hyderabad

Email: mallesh67@gmail.com

Abstract

This project presents a new cryptographic technique intended to improve the security of using TCP and UDP protocols to send data to a target device. They want to develop a novel approach to cryptography that offers a high degree of security by sending messages via the MAC address of the target device. Utilize the suggested algorithm to compare the TCP and UDP protocols. Efficiency, velocity, caliber, and mistake rate The main goal of this project is to provide a mechanism that can obfuscate a message's meaning by encoding it in characters that cannot be printed. To achieve this, the algorithm employs a combination of random integer keys and ASCII conversions, rendering the encrypted message nearly impossible to decipher without the proper decryption process. The first step in the suggested encryption technique is to convert the message contents into the appropriate ASCII values. The ciphertext is then created by further obscuring these ASCII values using a random number. The final ASCII code is created by applying mathematical processes to strengthen security and protect the data from unwanted decoding. The message format at the sender's end consists of the text to be encrypted, a random number, and the recipient's MAC address. This composition is sent to the recipient as ciphertext after being encrypted. The decryption procedure starts as soon as it is received. To confirm authorization, the MAC address must first be decrypted. In the event that decryption is successful, the ciphertext is used along with the random number as the decryption key until the entire original message is rebuilt. Importantly, this cryptographic algorithm is versatile and can be applied to both TCP and UDP protocols, serving as the encryption mechanism at the sender side and the decryption process at the receiver side, at the final result we get more security and high level of authentication, the technologies environment of the project in java language using windows 10 with RAM 8 GB and COR I5 and the result depend on this environment.

Keywords: encryption, decryption, algorithm, cryptography, MAC address, TCP, UDP, ASCII, random numbers, security, ciphertext

1. INTRODUCTION

A crucial part of computer security is cryptography, which uses sophisticated encryption methods and mathematical algorithms to prevent unwanted access to digital data. It is employed to guarantee the secrecy, integrity, and validity of data as well as to transform readable information into unreadable text. An overview of cryptography and its uses in the military, banking, and internet communications is given in this paper. It also covers message authentication techniques and digital rights management systems. This presentation concludes by summarizing the role that cryptography plays in computer security and how it can be used to prevent unauthorized access to digital data.

Sensitive information must be protected from malevolent attackers via data encryption. It uses a method known as ciphertext to jumble data into an unintelligible format. Using a key, decryption is the process of returning encrypted material to its original form. The methods of encryption and decryption, their significance for preserving safe online communication, and their use in safeguarding personal information are all covered in this essay. It also sheds light on possible security dangers connected to data encryption.

Data can be protected and made accessible to only those with the encryption key by using the processes of encryption and decryption. Organizations in charge of intelligence and security use it for a variety of purposes, including personal security. This technique is used by software to shield people from possible dangers. This paper presents a new algorithm that allows messages to be hidden in unreadable characters using multiple random number keys and ASCII conversions. This document aims to guarantee that the message is secure and encrypted, rendering it unintelligible to outside parties. Additionally, it seeks to guarantee the highest levels of security for the message. The algorithm proposed in this paper can be implemented in several ways. For example, it can be used to encrypt large amounts of data that need to be protected from unauthorized access. The algorithm can also be used to securely send messages over the Internet, ensuring that only the intended recipient can read the message. Additionally, the algorithm can be used to create a secure tunnel for the communication of sensitive data. Finally, the algorithm can be used to create a secure file system, ensuring that only authorized individuals can access the stored data. In addition, the algorithm can be applied to various other applications, such as authentication and authorization systems, where it can be used to protect user credentials. Furthermore, the algorithm can be used to securely store passwords, preventing them from being accessed by unauthorized individuals. Moreover, the algorithm can be used to encrypt data stored in databases, ensuring that only authorized users can access the data. Finally, the algorithm can be used to securely transmit data over the Internet, ensuring that only the intended recipient can access the data.

This paper presents a new cryptography algorithm that uses the MAC address of a target device to send encrypted messages. The proposed algorithm is applied to the TCP and UDP protocols to compare their efficiency, speed, quality, and error rate. The results of the comparison will be used to evaluate the effectiveness of the proposed algorithm in providing a higher level of security.

This paper presents a new cryptography technique that utilizes ASCII values and random numbers to create secure ciphertext. By including the MAC address of the receiver in the message format, the proposed algorithm ensures authorization and prevents unauthorized access. The encryption and decryption processes are applied to both TCP and UDP protocols at the sender and receiver sides, respectively. The mathematical operations used to produce the final ASCII code further enhances the security of the data from potential intruders.

2. LITERATURE SURVEY

Cryptographic Algorithm Based on ASCII and Number System Conversions along with a Cyclic Mathematical Function

This paper presents a new cryptology algorithm for data encryption and decryption. This algorithm provides comparatively higher security of data by converting plaintext into unprintable characters. The steps of the algorithm involve conversion of plaintext into its equivalent ASCII (decimal) numbers, which are further converted to its equivalent octal and hexadecimal numbers, followed by matrix manipulation and cyclic mathematical function to form the intermediate and final cipher texts. The total 32 unprintable characters used in this algorithm make it difficult for intruders to break down the message with every possible combination and thus, provide higher level of security for real-time communication.

ASCII Based Cryptography Using Unique lei, Matrix Multiplication and Palindrome Number

This paper proposes a new encryption technique, the UPMM algorithm, which applies an ASCII value to data to be encrypted. The encryption key involves palindrome numbers and a unique alphanumeric ID, which is also converted into ASCII value for authentication over the network. The algorithm uses a mixture of palindrome numbers and matrix multiplication to encrypt the data, which is then sent over the network in sets of three keys. The receiver is then able to decrypt the data using the inverse of the encoding matrix. This approach is more secure than the existing methods of encryption using Armstrong numbers, as it makes it more difficult for a crypt-analyst to find the key.

A New Cryptography Algorithm Based on ASCII Code.

This paper presents a new cryptography algorithm which considers linking each character in the plaintext with its previous one during encryption and decryption. The algorithm is designed to protect user's data and infrastructure by providing strong security. It can be used to handle different situations in cryptography applications and has been tested with simulation results which demonstrate its effectiveness. The proposed algorithm can be used to increase the security of distributed systems and protect data from unauthorized access.

Cryptographic Algorithm Based on ASCII and Number System Conversions along with a Cyclic Mathematical Function.

This paper introduces a cryptology algorithm that provides a higher level of data security. The algorithm converts the plaintext into unprintable characters using a series of steps involving ASCII and number system conversions, matrix manipulations, and a cyclic mathematical function. The result is a long, secure encrypted message that would take a long time to break through with every possible combination. The length of the encrypted message is longer than the original message, but the increased security is worth it for real-time communications.

3. SYSTEM DESIGN AND ANALYSIS

In the above papers presents a novel data hiding technique based on a novel cyclic mathematical function and multiple ASCII conversions. Experiments have shown that it takes more time to encrypt and decrypt messages than other proposed methods, and that the technique requires higher CPU specifications. The algorithm includes several steps for higher security, but more steps result in more time and CPU resources being consumed. Furthermore, it is difficult to detect the existence of secret information, and brute-forcing the hash function is a difficult task. However, the length of the encrypted message is larger than the original message, which requires more space in memory. The proposed algorithm should be developed further to provide more robustness and support asymmetric encryption, IN the next chapter a new algorithm for cryptography that uses unprintable characters in order to hide the meaning of a message. The algorithm works by converting data into its respective ASCII values and then converting those values to cipher text using a random number. Mathematical operations are also used to produce a final ASCII code for extra security. The message sent by the sender includes the receiver's MAC address, a random number, and the text to be encrypted. The receiver will decrypt the MAC address to ensure authorization and then continue to decrypt the ciphertext using the random number until the original message is obtained. This algorithm can be applied to both the TCP and UDP protocols and is used for encryption at the sender side and decryption at the receiver side.

4. PROPOSED ALGORITHM

Proposed algorithm

A new cryptographic algorithm is presented in this project to increase security. This method makes it feasible to conceal a message's meaning in characters that cannot be printed. The main goal of this work is to use a variety of random integer keys and ASCII conversions to make the encrypted message irrefutable unprintable. This project's goal is to suggest a novel form of cryptography. It transforms the data into its corresponding ASCII values, and then employs a random integer to translate these ASCII values into cypher text. The process also employs mathematical operations to generate the final ASCII code, which protects data from being encrypted by others. near the sender side the format of the message include the MAC address of receiver, random number and text, which be encrypted to produce chipper text, then the sender will send chipper text to receiver, At the receiver side the first process of decryption is to decrypt the MAC address to see is matched or not to achieve authorization, then if it matches will continue decrypt chipper text through key of the random number until obtain the original message.

This algorithm which be applied for TCP and UDP protocol at sender and receiver side. At sender: encryption and At receiver: decryption. This work suggests a brand-new cryptography algorithm. that uses unprintable characters in order to conceal the message's significance. The algorithm operates by translating input into its corresponding ASCII values and then utilizing a random integer to turn those values to encrypted text. For added security, mathematical techniques are also performed to create the final ASCII code. . The message sent by the sender includes the receiver's MAC address, a random number, and the text to be encrypted. The receiver will decrypt the MAC address to ensure authorization and then continue to decrypt the ciphertext using the random number until the original message is obtained. This algorithm can be applied to both the TCP and UDP protocols and is used for encryption at the sender side and decryption at the receiver side.

Aims of proposed algorithm

1. Create a new methodology of cryptography which provide high security level by using target device MAC address to send a message
2. Apply proposed algorithm in TCP and UDP protocols to compare between them

Efficiency - Speed - Quality - Error rate

5. RESULT

Discussion of the algorithm's output

Encryption Time in	Decryption Time in	Length of the message+ MAC	Message

milliseconds	milliseconds	address	
114	320	16	AaZa19
552	538	26	MohammedYass1995
991	541	36	1234567890MohamedYas1995
754	1422	46	1234567890/*-+!@#$%^MohamedYas1995
778	540	56	1234567890/*-+!@#$%^ MohamedYas1995HELLOAhmed

Table 4: Encryption and Decryption Times

A user has encrypted five different messages with varying lengths and MAC addresses. The timing of each message's encryption and decryption is recorded in the table above. From the table, we can conclude that encryption and decryption taken time of a message increases with the length of the message. The longer the message, the more time it takes to encrypt and decrypt it. The MAC address also affects time required to encrypt message and decrypt a message, as messages with longer MAC addresses take longer to encrypt and decrypt.

Discussion of the algorithm's output using TCP protocol

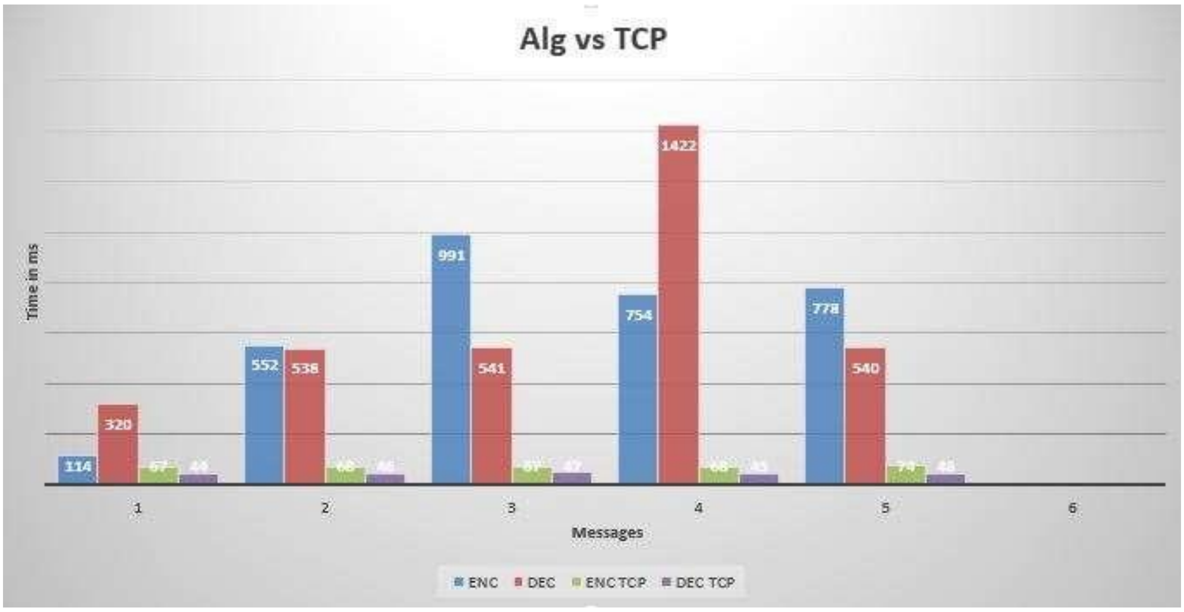

Figure 1: apply algorithm in TCP

From the data in the above figure, it can be concluded that the encryption and decryption times increase with the length of the message. The encryption time at the sender is slightly higher than the decryption time at the receiver and both of encryption and decryption using TCP are less than algorithm.

Discussion of the algorithm's output using UDP protocol

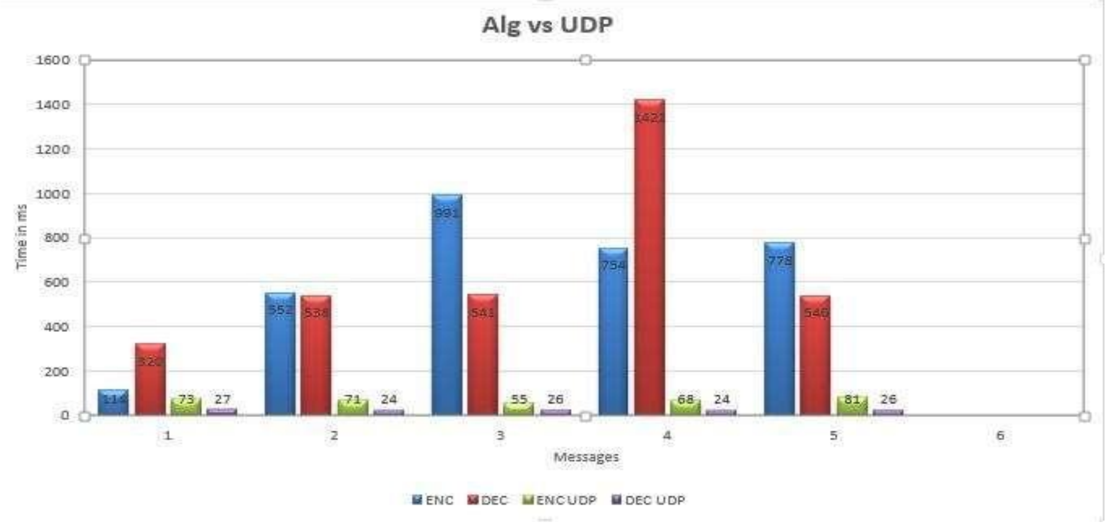

Figure 2: apply algorithm in UDP

From the table longer messages require longer encryption and decryption times at both the sender and receiver. The encryption time at the sender and the decryption time at the receiver both rise as the message length increases.

	algorithm's output	algorithm's TCP output	algorithm's UDP output
Efficiency	Determined by the size of the secret key and can be improved by using faster algorithms and optimization.	Efficient for secure communication.	UDP is more efficient but less reliable than TCP.
Speed	The size and type of encryption algorithm used will affect the speed and complexity of the decryption process.	The algorithm is fast and secure, making it an ideal choice for secure communication.	UDP being faster
Quality	Strong encryption algorithms are essential for a secure and reliable algorithm.	This algorithm provides a secure and reliable way to send encrypted messages, ensuring the message is only read by the intended recipient.	UDP being more efficient but less reliable than TCP.
Error rate	The error rate of an encryption algorithm depends on its strength.	The proposed algorithm provides a secure and reliable communication system with low error rate.	UDP has higher error rate but is more efficient than TCP.
Brute force	Brute force is a time consuming and	Low brute force risk.	Robust system for protecting messages

	challenging method of finding a secret key.		from unauthorized access.

Table5: compare between tcp and udp

Comparison between TCP and UDP protocols

The comparison between the two tables shows that TCP encryption and decryption times are generally faster than UDP encryption and decryption times. This is because TCP provides a more reliable connection, as it requires acknowledgement of data packets from the sender to the receiver. UDP is not as reliable because it does not require acknowledgement of data packets and therefore is less reliable. In the first table, the encryption and decryption times for TCP range from 67-68 milliseconds at the sender and 44-47 milliseconds at the receiver, with the longest message taking 74 milliseconds at the sender and 46 milliseconds at the receiver. In the second table, the encryption and decryption times for UDP range from 73-81 milliseconds at the sender and 27-26 milliseconds at the receiver, with the longest message taking 81 milliseconds at the sender and 26 milliseconds at the receiver. Overall, the encryption and decryption times for TCP are faster than those for UDP, indicating that TCP provides a more reliable connection than UDP.

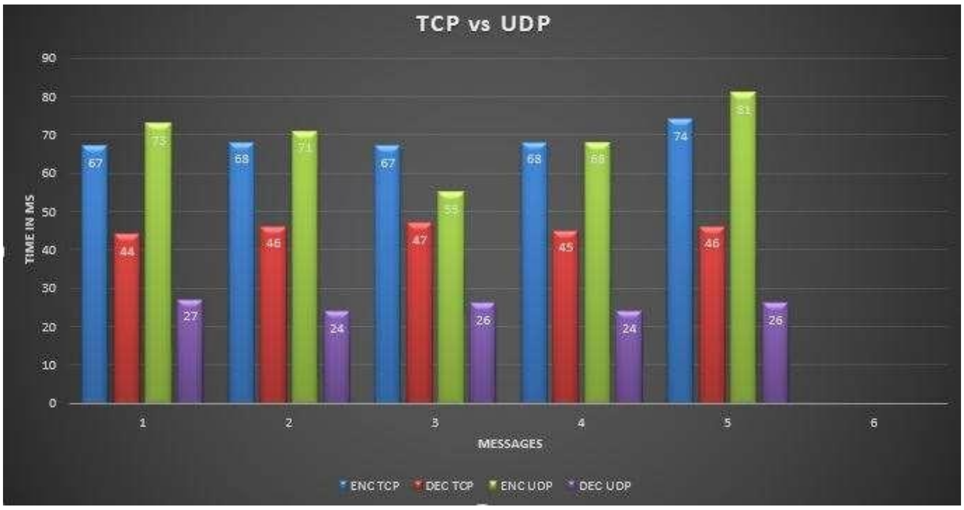

Figure 3: TCP vs UDP

CONCLUSION

The Send Encrypted Message to a Target Device Algorithm (SEMTDA) provides an extra layer of security for data and communications by using a MAC address of a target device as a key for encryption. The encryption method used is strong enough to make it virtually impossible for any other device to crack the code and access the message. Additionally, using the User Datagram Protocol (UDP) instead of the Transmission Control Protocol (TCP) can provide additional benefits in terms of speed, reliability, and security. As a result, the SEMTDA algorithm is a powerful tool for ensuring the security of data and communications.

Reference

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

[2] Sidhpurwalahuzaifa. A Brief History of Cryptography. [Online]. Available:

https://securityblog.redhat.com/2013/08/14/a-briefhistory-of-cryptography/

[3] A. Menezes, V. Oosrschot and A. Vanstone, Handbook on Applied Cryptography, CRC Press Inc., NY,USA, 2000.

[4] D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.

Text Books:

1. Computer Networks, Andrews S Tanenbaum,, Edition 5, PHI, ISBN:-81-203-1165-5
2. Computer Security - Principles and Practices (Except the Chapters 13, 14, 15, 16, 17,18, 19), 2nd Edition by William Stallings, Pearson Education,Inc.