International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Stability Analysis and Controlling MITM Attack in Dynamic Network

Mrs. R. Ramya[1], N. Sriram[2], S. Suryanarayanan[3]

[1]*Assistant professor, Department of computer science, Jeppiaar SRR Engineering College*
[2,3] *Student, Department of computer Science, Jeppiaar SRR Engineering College*

Abstract - *The communication channels may be subjected to malicious attacks, which will destroy the communication links and result in disconnected topology of the communication networks. The impacts of attacks on different communication networks are different and independent. To overcome this problem, MITM defence technology is used. The method to improve network speed and cryptography, the HONEY algorithm technique have been proposed and analysed.*

Key Words: MITM Attack, MITM defence, AES Algorithm, Honey Algorithm

1. INTRODUCTION

In computer networks, exchange data with each other using connections between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

It considers here the scenario that the communication channels for controllers and observers may be subjected to frequently malicious attacks, which will destroy the communication links and result in disconnected topologies of the communication networks. It is assumed that the impacts of attacks on different communication networks are different and independent. New security control strategies are proposed and analysed. An algorithm to properly select the feedback gain matrices and coupling strengths is presented. By utilizing the Lyapunov stability theory, sufficient conditions are derived to check whether final consensus tracking can be achieved against such[1] attacks. Finally, a simulation example comparing the security control and uncontrolled scenarios is demonstrated to show the effectiveness of the theoretical results.

The AES is often called as a one-way function because from the cipher text the plain text cannot be retrieved from the guess made by any other attacks. Thus, the AES algorithm is an effective one which could be used for effective encryption techniques. But the problem here is that the AES algorithm is affected by the brute force attack and also by many side channel attacks. So, honey encryption has to be used. The honey encryption is the technique which is used to cheat the hacker with the generated fake message which looks like a real one, so the attacker got confused of choosing the correct key. The AES hardware mode is also changed in [2] to reduce the cost of implementation of AES.

2. RELATED WORK

The advanced encryption standard (AES) is mentioned as the best standard encryption algorithm by the US government, but there is one major attack on the AES that is the brute force attack. In this project, the description of the AES, honey encryption and the methods to improve its speed and performance than the honey technique. The only point where AES algorithm failed was Brute Force Attack.

The honey concept in the visualization concept; that is, if a hacker tries to attack the system in an organization, then this concept will wrongly redirect the hacker to go for some other system. It also made the hacker to believe that the redirected system is what the attacker wants. So, the hackers are cheated, and the attack from the key puncher is prevented.

3. PROPOSED WORK

The existing systems uses AES algorithm for encryption and decryption the actual data. The major aim of these systems is to improve the network. And also make sure that it's not crack able since the combinations of keys are massive. The only point where AES algorithm failed was Brute Force Attack.

AES algorithm failed in Brute Force Attack, So new security control strategies HONEY algorithm is used .A brute force attack is a trial-and-error method used to obtain information by guesses as to the value of the desired data. The algorithm is about to speed the network and reduce the attack. Honey concept in the visualization concept, this will wrongly redirect the hacker to go for some other system. It also made the hacker to believe that the redirected system is what the attacker wants.

3.1 GENERAL ARCHITECHTURE

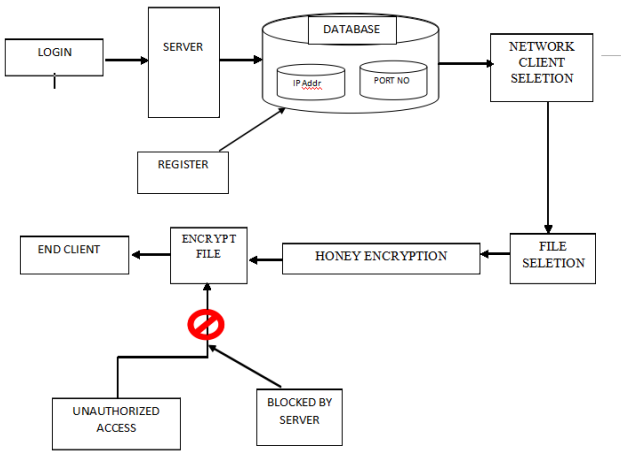

Figure 1 General Architecture Diagram

Users can registers by giving their details and their port number. All their details are passed to the admin. Database contains IP address data and port number data stored after completion of registration. After registration user can login, than user can see the other entire user who are all connect with in the network.

The user can connect with other users with help of connection option and this is the network client selection. After establishing the communication, select the file that to be send. Send that file to the connected users and at the same time the random key is generated. Encryption and decryption is done by the honey encryption algorithm. Then the user can send the file to selected user. In client side the user get the file and use that secret key to encrypt the decrypted data.

If unauthorized users try to access the encrypted file what to type random key to decrypt the file. If user types wrong password then notification send to server. when server got notification block the user form the network. After the blocking the user cannot enter into the network again.

3.2 ADVANTAGES OF PROPOSED WORK

The brute force attack is controlled by the honey encryption algorithm. So the user cannot try the password in guessing. Honey Encryption could help reduce their vulnerability and to protect data stored on password manager services. The unauthorized user cannot get the original content of the file, but they get a fake file. The unauthorized user will think that the retrieve data is the original content.

4. MODULE DESCRIPTION

4.1 CLIENT SELECTION NODE

It can learn all the subsequence sessions. If an client and an storage device complete matching sessions, they compute the same session key. Here the connection establishment is done. So we can select the IP address for which we are going to send the sensitive data.

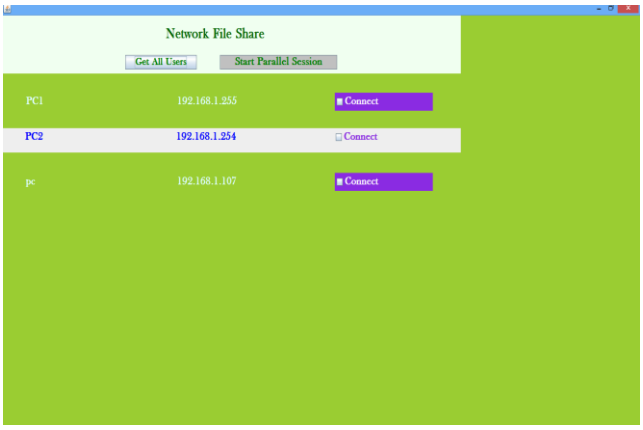

Figure 4.1 client node selection

4.2 RANDOM KEY GENERATION

To design efficient and secure authenticated key exchange protocols [5] and give some intuition of a variety of pNFS authenticated key exchange protocols. After selecting the receiver IP address, the random key is generated for the transmission of the sensitive data.

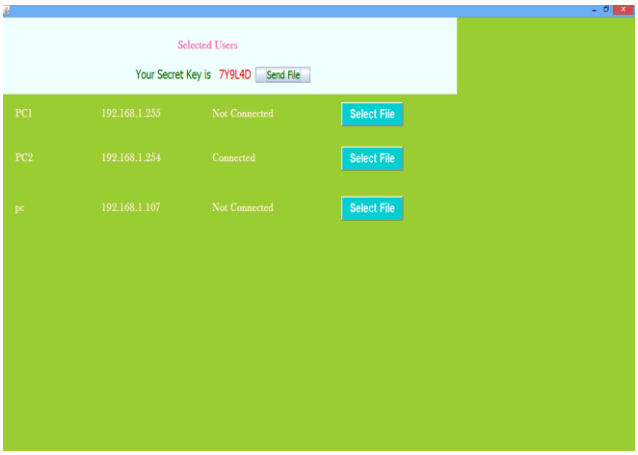

Figure 4.2 File selection

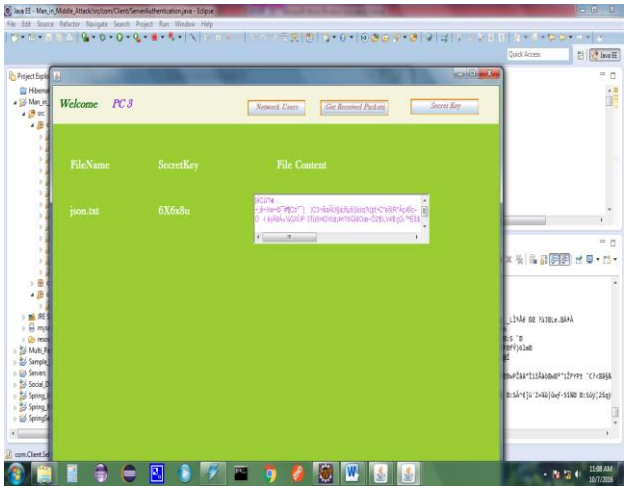

Figure 4.3 Honey encryption

4.3 MITM ATTACK

In this module the unauthorized user i.e., the users who are not having permission to access other information. The user who uses the network in a wrong manner may block by the server when the server gets a notification message that someone is accessing in unauthorized access. Once the Unauthorized user blocked by the server cannot be undone ever.

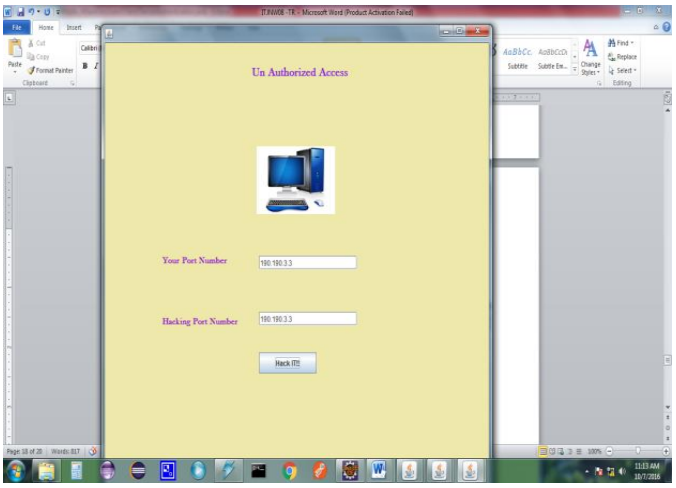

Figure 4.4 MITM attack

4.4 MITM DEFENCE

The admin can accept the new user request and also block the users. The users can upload the file to Network. And the admin can allow the files to Network then only the file can store the cloud. If the file uploaded by the user is not permitted from the Server means the file cannot be uploaded by the Client.

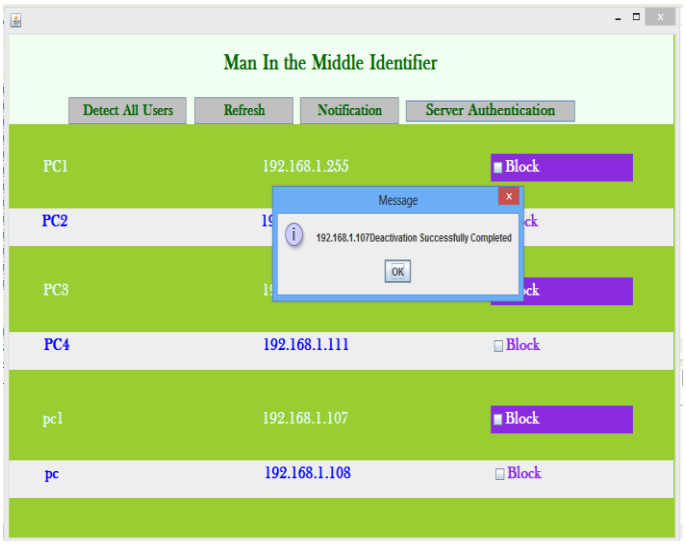

Figure 4.5 MITM defense

5. CONCLUSION

Honey encryption algorithm can be used to eliminate the drawback of the AES algorithm. The brute force attack is the major problem which is eliminated and the difficulty in the field of the key management can be removed effectively by using the honey-word generation algorithm. Also, we provided various MITM defense mechanisms along with their descriptions.

REFERENCES

[1] Ying Wan, Jinde Cao and Guanrong Chen "Distributed Observer-Based Cyber-Security Control Of Complex Dynamical Networks", IEEE Transactions on circuit and systems, Volume 64, Issue 11, pp. 851-826, August 2017.

[2] Deguang Le, Jinyi Chang, Xingdou Gou and Ankang Zhang,"Parallel AES algorithm for fast Data Encryption on GPU", IEEE Transactions on *Computer Engineering and Technology*, Volume 23, Issue 18, pp. 243-277, June 2010.

[3] Arokia Renjith J and Mohan kumar P, "Screening the covert key using honey encryption to rule out the brute force attack of AES", IEEE Transactions on security, Volume 9, Issue 18, pp. 544-556, May 2016.

[4] Aris Juels A and Ristenpart T, "Honey encryption: encryption beyond the brute-force barrier", IEEE Transactions on Security & Privacy , Volume 12, Issue 4, pp. 546-576, August 2014.

[5] N.Narmadha and S. Rajathi, "Password-Only Authenticated Key Exchange Using Distributed Server", IEEE Transactions on parallel and Distributed Systems , Volume 24, Issue 9, pp. 157-176, June 2014.

[6]Mihir Bellare, David Pointcheval and Phillip Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks", IEEE Transactions on computer security , Volume 12, Issue 17, pp. 75-103, March 2013.