Secure Data Transmission in MANET

Vaishnavi Kanta, Sneha Singh, Sakshi
Galgotia College of Engineering and Technology
Knowledge Park-1, Greater Noida

Sandhya Katiyar, PhD
Associate Professor
Galgotia College of Engineering and Technology
Knowledge Park-1 , Greater Noida

ABSTRACT

Network Security is a complex subject that can be intercepted by well versed and skilled people.Today, with increase in networking, the folks need to know the importance of security in network. Cryptography is a field for providing security to the networks and protecting information and communication. Even after providing securities, the network is vulnerable to some of the attacks in different networking areas like Man-in-the middle attack in the area of key exchange protocol.. Statistical tests are used to check these sequences, before calculating the private key and the shared key. In the paper, the generated binary sequence is converted into Octal instead of Decimal so that the memories utilized by both the generated keys are reduced and the complexity is decreased. Decimal sequence is of 10 bits whereas octal sequence is of 8 bits, so changing the sequence to Octal instead of Decimal will result in the reduction of 2 bits which may eventually reduce the complexity and memories utilized. Also, converting the binary sequence to octal allows the password to be minimum 128-bits . Previously, the password was set to the limit 256-bits range but now the limit is lowered to 128-bits range. In future, this method can be implemented on other encryption methodologies to provide a secure environment for secure transmission of data.

Keywords

Diffie-Hellman, network security, complexity

1. INTRODUCTION

Now a day, wireless transmission of data has become very fast due to internet. Any size and type of data can be sent via internet and at faster rate. As the transmission of data via internet is fast, it is also not secure. It is necessary to protect the data from the unauthorized access. There are various techniques that can be used to secure the data like, cryptography and steganography. Cryptography is a technique that protects the data by encoding it.Cryptography is also used with biometrics in some of its modifications which new to knowledge[8].

Cryptographic algorithms are broadly categorized as symmetric and public key cryptography. In symmetric key cryptography Single key is used for encoding and decoding where as in public key cryptography two keys are used, public key and private key [1]. Symmetric key should be changed continuously at some time interval to make it secure and prevent unauthorized users from accessing the data.Cryptography is logic of mathematical manipulationof data (cipher text) with some text (Key)[9]. Therefore, the security of any symmetric cryptography system depends on the key exchange protocol. Key exchange protocol is the mechanismof distributing the keys between the users in secure way [2].

Diffie-Hellman key exchange is a cryptographicprotocol in which two parties exchange their shared keys over an insecure channel. This key exchange protocol does not provide authentication of the parties involvedand is thus vulnerable to Man-in-the-middle attack [3].One of the major problem of this protocol is that an attacker can attack and intercept the communication and behaves as sender for the receiver and vice versa. At the end both the parties share the secret key with the attacker, which ends up with the full access to the communication over the channel[7].

Diffie-Hellman Key-Exchange Protocol is used for sharing secret key between users when more than one attacker are present between sender and receiver[14].Compression is the process of reducing the number of bytes or bits needed to represent a given set of data. It helps in saving more data[15].

In this paper, the focus is on the generation of keys by using the binary sequence of higher bits and converting the resulting binary sequence to octal instead of decimal to make it more efficient which will simultaneously solve the security problems and prohibit an intruder to eavesdrop.

2. OVERVIEW

2.1 Man-in-the-middle Attack

Man-In-The-Middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems. It is one of the main threats to the wireless data communication. In this, the communication is intercepted by the outside entity. MITM attacks target the actual data that flows between endpoints, the integrity and the confidentiality of the data itself [13]. The message being transferred from the sender to the receiver is accessible by the attacker. The attacker, after having access to the information can read, intercept or modify the information. There are four basic types of Man-in-the-middle attack.

First is, Spoofing-based Man-in-the-middle attacks in which the adversary intercepts the legitimate traffic with the help of spoofing attack and controls the data transmitted without hosts being aware of adversary existence. In case of DNS spoofing, adversary spoofs devices between the end points and in case of ARP spoofing, adversary directly spoofs these end-points or the victim’s devices. Second is, SSL/TCL Man-in-the-middle attacks in which the adversary inserts itself in the communication channel between the two end points or the victims. Adversary establishes two separate SSL connections and relays messages amongst them. Thus the adversary can record all the messages and also selectively modify the data. Third is, BGP Man-in-the-middle attacks in which adversary delivers the stolen traffic to the destination. This is IP hijacking where the traffic passes through autonomous station of the adversary, where there are chances of traffic being manipulated. Fourth is, the false base station Man-in-the-middle attack in which the adversary create a fake transceiver station and then use them to manipulate the victim's traffic [4].MITM attack can successfully invoke attacks such as , and Port stealing, DNS spoofing, Denial of service (DoS)[12].

2.2 Diffie-Hellman key exchange protocol

Diffie-Hellman introduced the first Key exchange protocol. Diffie-Hellman does not authenticate the communicating entities itself [10].Diffie-Hellman key exchange protocol is a protocol in cryptography in which transmission of data over an insecure channel takes place between sender and receiver by using a shared secret key. The sender and receiver do not know each other. The Diffie-Hellman key exchange does not provide authentication of the communicating parties and is thus susceptible to man-in-the-middle attack [3].Diffie-Hellman key exchange are also called exponential key exchange. It is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys[11].

For example, To implement Diffie-Hellman, the two end users joey and kabe, while communicating over a private channel, mutually agree on positive whole numbers m and n, such that m is a prime number and n is a generator of m. The generator n is a number that, when raised to positive whole-number powers less than m, never produces the same result for any two such whole numbers. The value of m may be large but the value of n is usually small. Once joey and kabe have agreed on m and n in private, they choose positive whole-number private keys j and k, both less than the prime-number modulus m. Neither user discloses their personal key to anyone. Next, joey and kabe compute public keys j* and k*. The two users can share their public keys j* and k* over a communication medium that is assumed to be insecure, such as the Internet or a corporate WAN. With the help of these public keys, a number z can be generated by either user on the basis of their own personal keys. The value of z turns out to be the same according to either of the two. However, the personal keys j and k, which are critical in the calculation of z, have not been transmitted over a public medium [5].

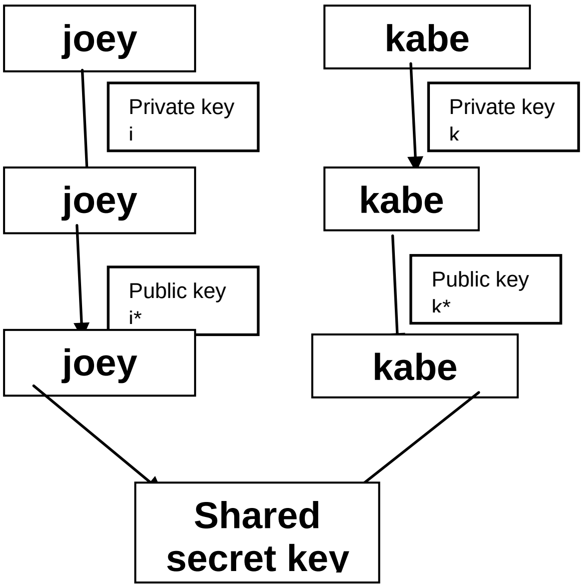

Figure.1 Diffie-Hellman key exchange process

3. EQUATIONS

Diffie-Hellman key exchange protocol is basically based on mathematical equations for the determination of their public key and shared secret keys.

Joey and Kabe compute public keys j* and k* based on their private keys j and k according to the formula,

$j^* = n^j \bmod m$

and,

$k^* = n^k \bmod m$

Joey then computes the value of z using the formula

$$z = (k^*)^j \bmod m \qquad (1)$$

Bob computes the value of z using the formula

$$z = (j^*)^k \bmod m \qquad (2)$$

The value of z in equation (1) and (2) are same, the resultant shared secret key.

4. LITERATURE REVIEW

[1] *R.Pranesh, V.Harish, M.Vigneshwaran, G.Manikandan, "A New Approach for Secure Data Transmission", 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].*

When the data is transfer from one medium to another medium then security play a vital role on the private data over the communication medium which tends to be open and insecure. For secure the data from the intruder they used the RSA algorithm. RSA algorithm mainly has been used for secure data transmission. In a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret.

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

Decryption is a process in which the conversion of encrypted data into its original form and it is a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

[2]*Aqeel Sahi Khader, David Lai, "Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol", 22nd International Conference on Telecommunications (ICT 2015).*

Cryptography or cryptology is the study of techniques for secure communication in the presence of third parties called adversaries. It mainly secures the data from the public reading private messages. Here, uses the two method i.e. encryption and decryption in which to secure the data we uses the public key and the private key. Public key is for everyone but the private key is a secret key or password which is mainly known by the authorized user.

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

[3] *Nan Li, "Research on Diffie-Hellman Key Exchange Protocol", 2010 2nd International Conference on Computer Engineering and Technology, pp. Volume 4-634-637.*

Diffie-Hellman key exchange (D-H) is a Cryptographic Protocol. It allows two parties that have no prior knowledgeof each other to establish together a shared secret key over an insecure communications channel. The protocol is limited to exchange of the keys. There is no entity authentication mechanism in this protocol, because of which it is easily attacked by the man-in-the-middle attack and impersonation attack in practice.The computational efficiency of various authentication methods is compared.Finally an improved key exchange schema based on hash function is given, which improves the security and practicality of Diffie-Hellman protocol.

By simulating the various key exchange processes based hash function, public-key encryption and Symmetric-key encryption within the LAN, we can see that the hash function's efficiency is more effective than the symmetric-key encryption algorithms for small message, such as MD5 algorithm's speed is about 5 times faster than the DES algorithm's speed and SHA-1's speed is more twice than the DES's speed. Because of including the authentication mechanism, the improved Diffie-Hellman key exchange protocol can resist man-in-the-middle attack, impersonation attack and replay attack..The authentication using hash function has less computing quantity and the faster computing speed than the other public key and symmetric key encryption algorithm.

[4] *Bharat Bhushan, G Sahoo, Amit Kumar Rai, "Man-In-The-Middle Attack in Wireless and Computer*

Networking- A review", 2017 IEEE

Man-in-the-Middle attack is one of the primary threats against wireless network security.It is the most successful attack that is launched for gaining control over the transferred sensitive end users.In this, the attackers target the actual data flowing between the endpoints and also compromise the integrity and confidentiality of the data.Adversary can modify, intercept or destroy the messages to cause end of communication for one of the parties thereby leading to compromise of availability issue. MITM attacks can be launched in various communication channels including UMTS, long term evolution, GSM, Wifi and Bluetooth. MITM attacks are basically divided in four basic types- Spoofing-based MITM attacks, SSL/TSL MITM attacks, BGP MITM attacks, false base station MITM attack.Prevention mechanismsfor all such attacks is presented.OSI reference model and two basic networking technologies such as GSM and UMTS is considered.

[6]*S. M. Hosseini, H. Karimi, and M. V. Jahan, "Generating pseudorandom numbers by combining two systems with complex behaviors,"Journal of Information Security and Applications, pp. 149–62, 2014*

Cellular automata (CA) have many applications due to its complex behavior such as generating random numbers and cryptography. A long sequence of random numbers cannot produce a pure CA. In order to to generate random numbers, a non-uniform CA as a random number generator has been combined with Langton's ants. Langton's ant is a simple discrete dynamical system, with a surprisingly complex behavior.Langton's ants not only determine the CA rules but also give a random state to cellular automata by disordering its state The combination of some Langton's ants gives them a chaotic behavior and combination of this behavior with complex behavior of cellular automata causes a great efficiency in generating random sequences. Langton ants move on a square grid with white and black cells that still its simplicity has a random behavior. Cellular automata are updated by new selection rules and finally ants move one step forward. The results shows that the proposed generator has the maximum entropy and passes several statistical tests.

[7] *Kapil M. Jain, Manoj V. Jain , Jay L. Borade " A Survey on Man in the Middle Attack" , IJSTE-International Journal of Science Technology &Engineering , 2016*

Man in the middle attack allows the attacker to gain unauthorised entry into the connection between the devices which are connected. The man in the middle attack focuses on the execution of man in the middle attack on Diffie Hellman and what are the different methods with which it can be performed and the various defenses against the attack.

[8]*Abhishek Bhardwaj, Subhranil Som "Study of Different Cryptographic Technique and Challenges in Future" ,1st International Conference on Innovation and Challenges in Cyber Security (ICICCS)2016*

In this, history of all the data hiding techniques used in the history and how these techniques have evolved from Caesar cipher to DES and then to Triple-DES, AES and current algorithms are described.

[9] *Dudhatra Nilesh, Prof. Malti Nagle "The New Cryptography Algorithm with High Throughput", International Conference on Computer Communication and Informatics (ICCCI -2014), Coimbatore*

In this, new cryptography algorithm (Encryption and Decryption) has been generated and are compared by using some components like throughput of key generation, to generate Encryption text and to generate Decryption text.

[10] *Manoj Ranjan Mishra, Jayaprakash Kar " A STUDY ON DIFFIE-HELLMAN KEY EXCHANGE PROTOCOLS" ,International Journal of Pure and Applied Mathematics, 2017*

Diffie-Hellman introduced the first Key exchange protocol. Diffie-Hellman does not authenticate the communicating entities itself. A Key exchange protocol is the cryptographicprimitive that can establish a secure communication.

[11] *K.Suganya , K.Ramya "Performance study on Diffie Hellman Key Exchange Algorithm" International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2014*

It provides a security improvement that makes the Diffie-Hellman key agreement and encryption scheme more secure against attacks, such as the known plaintext attacks, it suggests the use of randomized parameter in both schemes.

[12] *Gopi Nath Nayak ,Shefalika Ghosh Samaddar "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions ", Department of Computer Science and Engineering Motilal Nehru National Institute of Technology ,Allahabad*

MITM attack has lot of surprising consequences in store for users such as, stealing online account password, userid, stealing of local ftp id, ssh or telnet session etc.MITM attack can successfully invoke attacks such as Port stealing, Denial of service (DoS) and DNS spoofing.

[13] *Sonia Rachel, Subhashkar S ," An Overview of the Man-In-The-Middle Attack", National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS), 2017*

MITM attacks target the actual data that flows between endpoints, the integrity and the confidentiality of the data itself. The MITM attack makes it hard for the clients to comprehend on whether or not they are associated with a unique and a secured connection.

[14] *Sulochana Devi, Ritu Makani ,"Encoding N-party Man-In-Middle Attack for Diffie–Hellman Algorithm in a Client-Server Paradigm", International Journal of Computer Science and Information Technologie (IJCSIT),2015*

Diffie-Hellman Key-Exchange Protocol is used for sharing secret key between users when more than one attacker is present between sender and receiver. It mainly focuses on generation of N-Party Man-in-Middle Attack in Diffie–Hellman Key Exchange Protocol.

[15] *Sarita Kumari " A research Paper on Cryptography Encryption and Compression Techniques", International Journal Of Engineering And Computer Science, 2017*

Cryptography is evergreen anddevelopments.Compression is the process of reducing the number of bytes or bits needed to represent a given set of data. It helps in saving more data.

5. PROPOSED WORK

Method described in the base paper ensures that the private keys will not be sent through the channels, and will be saved as hashes in the server in the form of password. The password is encrypted from binary to decimal which may increase the bit size and in order to prevent Diffie Hellman algorithm from man in the middle attack, they can occupy more memory space to key formation. Here, the password is converted in decimal from binary so by encrypting the password from binary to octal in place of decimal as there are chances that converting the password from binary to octal may decrease the bit size as octal consist of 0-7 and this may lead to less memory utilization and there may be decrease in the complexities.

6. ALGORITHM

1. Start
2. Read 8-character password from the user.
3. Convert the password to ASCII.
4. Convert the ASCII sequence to binary sequence..
5. Test the sequence using the statistical frequency test and, if the test passes, continue else Goto step 1 and ask the user to enter another password.
6. Convert the binary sequence into Octal.
7. Calculate private key j and k for both the users.
8. Send authentication message to both the users.
   If authentication is received then continue, else exit.
9. Hash the Pw1 and Pw2 using Private key j and k.
10. Using m (prime number), n (base) and private keys j and k, calculate j*= n^j mod m
    k* = n^k mod m.
11. Calculate shared key using the public keys j* and k*, calculated in step 10,
    Z=k*^jmodm z= j*^k mod m.
12. The shared key is generated.
13. Stop.

7. STATISTICAL FREQUENCY TEST

For every binary sequence, we expect that the sequence is 0's, and 1's, in different bit size ranges as cumulative sum of $\underline{+}$(16+(4*x)) where x ranges from 1 to 4 from different bi range. The purpose of this test relies on the number of 0, N0 and the number of 1, N1 in the sequence N, which we need to test. The static used is:

A= $\underline{(N0\text{-}N1)^{2}}$

N

To check whether the sequence passes this test or not, for

one degree of freedom, the value of X1 should be less than the acceptance threshold values of the test (X1 < 3.1825) [6].

8. RESULT

The given table, shows the results of statistical frequency test. The bits range of the test varies from 128 bits to 1024 bits the shortest successful length that ensures the correct result of 128 bit from the above table. It is illustrated that the frequency test increases as the size of bit decrease. The 128 bit sequence generated from the password chosen by joey is

0111011001100001011010010111001101101000011011100110000101110110011010010100000000110001001100
10 00110011001101000011010100110110

Table.1 the results of statistical frequency test

Length of Pseudo	**Value of statistical Frequency test**	**Degree of freedom**	**Acceptance threshold**
1024 bits	0.76562	1	3.1825
512 bits	1.53125	1	3.1825
256 bits	2.06640	1	3.1825
128 bits	2.52125	1	3.1825

Every 8 bit of the above binary sequence is converted into octal. As the result, these numbers are obtained

166 141 151 163 150 156 141 166 151 100 061 062 063 064 065 066

Now, the modular 10 of each octal number is taken. So, that each number is represented by single digit. Then, merge all the single digit number to 16 digits

6113061610123456

Now, assume that the user private key will be four digit and should be between 2 & p-2 where p is given by the server. Then the 16 digits is divided in 4 blocks and one number is taken from each block randomly (let us take the first 1 of each block then the private key would be J = 6013).

Similarly, kabe will also choose hi desired password and 128 bit sequence generated using kabe's password is

01110011011011100110010101101000011000010111001
10110100101101110011001110110100000100011001101
1100110000000110100001101010100110001

Every 8 bit of the above binary sequence is convertedinto octal. As the result, these numbers are obtained

163 156 145 150 141 163 151 156 147 150 043 067 060 064 065 061.

Now,the modular 10 of each octal number is taken. So, that each number is represented by single digit. Then merge all the single digit number to 16 digits

3650131670370451

Then, the 16 digitsis divided in 4 blocks and one number is taken from each block randomly (let the private key of kabe would be K = 3603).

After getting their private key, Joey and kabe get two number m & n where m is prime and n is the primitive root and these two number from along with the public key from server. Joey will receive Kabe's public key, m , n and username and similarly, Kabe will get Joey's public key m, n and username. They will be encrypted using receiver's private key and the private key should be less than the prime m. For instance, let p=10007 and g=5, then the public key will be 2391 for joey and 6241 for kabe which, after further computation will result in a common shared secret key 1324.

Table 8.2 Shared secret key generation using same password

Password of 1st user	**Password of 2nd user**	**Common Shared secret key**
sunshine@54673ita	robertbrown##1298	7609
sunshine@54673ita	robertbrown##1298	4182
sherlockholmes@1212	gettoknow@itb#followme	5659
sherlockholmes@1212	gettoknow@itb#followme	7037

9. CONCLUSION

A secure method to prevent diffie-hellman key exchange protocol from man-in-the-middle attack is described in this paper. Statistical frequency test is used to check the binary sequence, before calculating the private key and the shared key. In the proposed method the private keys will be saved as hashes. In this method, the binary sequence is converted into octal which allows the password to be of minimum 128 bits. In future, this method can be implementeds on other encryption methodologies to provide a secure environment for secure transmission of data.

10. ABBREVIATIONS

- DNS - Domain Name Server
- ARP- Address Resolution Protocol
- SSL- Secure Sockets Layer
- TLS- Transport layer security
- IP- Internet Protocol
- BGP- Border Gateway Protocol
- WAN- Wide Area Network
- LFSR- Linear Feedback Shift Registers

11. REFERENCES

[1] R.Pranesh, V.Harish, M.Vigneshwaran, G.Manikandan, "A New Approach for Secure Data Transmission",2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[2] Aqeel Sahi Khader, David Lai, "Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol", 22nd International Conference on Telecommunications (ICT 2015).

[3] Nan Li, "Research on Diffie-Hellman Key Exchange Protocol",2010 2nd International Conference on Computer Engineering and Technology, pp.Volume 4- 634-637.

[4] Bharat Bhushan,G Sahoo, Amit Kumar Rai, "Man-In-The-Middle Attack in Wireless and Computer

[5] Networking- A review",2017 IEEE.

[6] https://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange

[7] S. M. Hosseini, H. Karimi, and M. V. Jahan, "Generating pseudorandom numbers by combining two systems with complex behaviors,"Journal of Information Security and Applications, pp. 149–62, 2014.

[8] Kapil M. Jain, Manoj V. Jain , Jay L. Borade " A Survey on Man in the Middle Attack" , IJSTE-International Journal of Science Technology &Engineering , 2016

[9] Abhishek Bhardwaj, Subhranil Som "Study of Different Cryptographic Technique and Challenges in Future" ,1st International Conference on Innovation and Challenges in Cyber Security (ICICCS)2016

[10] Dudhatra Nilesh, Prof. Malti Nagle "The New Cryptography Algorithm with High Throughput", International Conference on Computer Communication and Informatics (ICCCI -2014), Coimbatore

[11] Manoj Ranjan Mishra, Jayaprakash Kar " A STUDY ON DIFFIE-HELLMAN KEY EXCHANGE

[12] PROTOCOLS" ,International Journal of Pure and Applied Mathematics, 2017

[13] K.Suganya , K.Ramya "Performance study on Diffie Hellman Key Exchange Algorithm" International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2014

[14] Gopi Nath Nayak ,Shefalika Ghosh Samaddar "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions ", Department of Computer Science and Engineering Motilal Nehru National Institute of Technology ,Allahabad

[15] Sonia Rachel , Subhashkar S ," An Overview of the Man-In-The-Middle Attack", National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS), 2017

[16] Sulochana Devi, Ritu Makani ,"Encoding N-party Man-In-Middle Attack for Diffie–Hellman Algorithm in a Client-Server Paradigm", International Journal of Computer Science and Information Technologie (IJCSIT),2015

[17] Sarita Kumari " A research Paper on Cryptography Encryption and Compression Techniques", International Journal Of Engineering And Computer Science, 201