ISSN:0975-9646

Sulochana Devi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4281-4285

Generation of N-party Man-In-Middle Attack for Diffie–Hellman Key Exchange Protocol: A Review

Sulochana Devi[#1] Ritu Makani[*2]

[#1]*Student of Masters of Technology, Department of Computer Science and Engineering*
Guru Jambeshwar University of Science & Technology Hisar, India

[*2]*Assistant Professor, Department of Computer Science and Engineering*
Guru Jambeshwar University of Science & Technology Hisar, India

***Abstract*— Diffie-Hellman algorithm is used for secret key generation. The purpose of the Diffie-Hellman protocol is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages. Man-in-Middle attack is the main problem of Diffie - Hellman algorithm. The main aim of this paper is to study and analyze Diffie–Hellman Key Exchange Protocol. In this paper we study of N-Party Man-in-Middle Attack in Diffie – Hellman Key Exchange Protocol.**

***Keywords*— Diffie-Hellman Algorithm, encryption, decryption, asymmetric, cryptography.**

I. INTRODUCTION

For the security of information, one has to be prevent it from unauthorized users access (confidentiality), prevent it from unwanted changes (integrity), and it should be available to its intended users (availability). This can be guaranteed by means of some protocols that make use of security primitives such as hashing, digital signatures and encryption. The concepts of public-key (asymmetric) cryptography were introduced by Whitfield Diffie and Martin Hellman, from Stanford University, Ralph Merkle, from the University of California at Berkeley. Diffie and Hellman worked on public key cryptography while Merkle provided his contributions on public key distribution. For better result they decided to work together. Then they published a paper, titled "New Directions in Cryptography" in 1976 [15]. This paper presented a new idea to the field of cryptography that is called Diffie-Hellman key exchange protocol.

This algorithm has a major weakness in the form of man-in-the-middle attack [5]. In this attack, a malicious third party (eavesdropper) retrieves sender's public component and sends his own public component to receiver. When receiver transmits his public key, third party interrupts and substitutes the value with his own public key and then sends it to sender. Now there is an agreement on a common secret key with third party instead of receiver. It is possible for third party to decrypt any messages sent out by sender or receiver. There may be many attackers between sender and receiver, so in this paper we study of N-Party Man-in-Middle Attack in Diffie – Hellman Key Exchange Protocol.

II. LITERATURE REVIEW

Literature review presents a number of approaches related with Diffie -Hellman Key-Exchange Protocol and provides the background to the research by describing what has been done in prior research.

Lein Harn [1] et al . This paper proposed three protocols that securely integrate Diffie–Hellman key exchange into the DSA. One-round protocol can be used in secure e- mail transmission. Two-round protocol provides authenticated key exchange for interactive communications. Three-round protocol provides authenticated, key confirmation and non playback key exchange for interactive communications.

Nan Li [4] et al. This paper states that because of having no entity authentication mechanism, Diffie Hellman protocol is easily attacked by the man in the middle attack and impersonation attack in practice. In this paper, we compare the computational efficiency of various authentication methods. Finally an improved key exchange schema based on hash function is given, which improves the security and practicality of Diffie-Hellman protocol. By analyzing the security of the Diffie-Hellman protocol, this paper presents an improved key exchange protocol based on random number sequence. This protocol use a hash function to achieve authentication is a relatively simple, economical and practical programs without additional public key infrastructure as a support. Because of including Authentication mechanism, the improved Diffie-Hellman exchange protocol can resist replay attack.

Barun Biswas [6] et al . In this paper a new technique is proposed in the field of cryptography. In the Diffie – Hellman, man in middle attack is the main problem. So in this paper a new technique is introduced, so that man in the middle attack can be eliminated. This approach would be such that the middle man could not change the key. In the proposed technique both sender and receiver use a secret number e as the base of the log. If in the middle the key is attacked and the key is changed not necessarily the base will be e. However we can't say that man in the middle attack can be fully eliminate because the base selected by the middle man can be same as e unfortunately. More over Diffie-Hellman cipher is a great algorithm and this technique is encouraged by Diffie-Hellman algorithm.

C. Krishna Kumar [7] et al. Several techniques have been proposed for the distribution of public keys. The ability to distribute cryptographic keys securely has been a challenge for centuries. The Diffie-Hellman key exchange protocol was the first practical solution to the key exchange dilemma. The Diffie-Hellman protocol allows two parties to exchange a secret key over unsecured communication channels without meeting in advance. The secret key can then be used in a symmetric encryption application, and the two parties can communicate securely. However, if the key exchange takes place in certain mathematical environments, the exchange becomes vulnerable to a specific man in the middle attack. This paper explores this man in the middle attack, analyze countermeasures against the attack. The easiest method is to force authentication prior to the key exchange. Sender double encrypts a message first with own private key and then with receiver's public key. This is a signed, secret version of the message. This signed message, together with sender's identifier, is encrypted again with private key of sender and, together with ID of sender, is sent to A. The inner, double- encrypted message is secure from the arbiter (and everyone else except receiver). However, A can decrypt the outer encryption to assure that the message must have come from original sender. A check to make sure that sender's private/public key pair is still valid and, if so, verifies the message. Then A transmits a message to receiver, encrypted with private key. The message includes ID of sender, the double-encrypted message, and a timestamp. This scheme has a number of advantages. First, no information is shared among the parties before communication, preventing alliances to defraud. Second, no incorrectly dated message can be sent. Finally, the content of the message will be secret. However, this final scheme involves encryption of the message twice with a public-key algorithm.

Shilpi Gupta [8] et al. In this paper main focus on asymmetric cryptography and proposed a novel method by combining the two most popular algorithms RSA and Diffie-Hellman in order to achieve more security. RSA algorithm is used as Public key cryptography method. It is widely used in Electronic commerce protocol .It has a public key and private–key. Public key is known to everyone and used for encryption and Private Key is used for decryption. The RSA algorithm can be used for both digital signatures and public key encryption. It is based on the theory of Prime Numbers. Its security is based on the difficulty of factoring large integers. The amount of time it takes to factor a number of x bits is asymptotically the same as the time it takes to solve a discrete log over a field of size x bits. DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. In our paper we use both RSA and Diffie-Hellman for providing more security. In this approach the Diffie- Hellman is not used only for key generation but also for the generation cipher text.

Ekta Lamba [14] et al. The man in the middle attack can be overcome with public key certificates and digital signatures. Another problem of D-H is the brute force attack .This attack can affect the D-H if small prime number is used. In this paper, it is tried to give focus on the hardness of key by using safe primes that makes it almost infeasible to calculate discrete logarithms & thus using that key for encryption and decryption of data so that we get better security. The Diffie - Hellman encryption algorithm is enhanced by adding some more security codes or changes in the current algorithm. In this paper, a new design for enhancing the security of Diffie Hellman algorithm is proposed. This approach design will not contradict the security of the original Diffie-Hellman algorithm by keeping all the mathematical criteria of Diffie- Hellman algorithm remain unchanged. It is tried to improve the security of Diffie-Hellman Algorithm by making the key harder by the use of safe primes.

Rohini [16] et al. This paper provides harder encryption with extend public key encryption protocol for security. Proposed work in this paper provides better security and implemented in any network. It enhanced the hardness of security by DH algorithm. The DH algorithm is improved by adding modulus operation on the private key. That increases the entropy and decrease the autocorrelation.

III. DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL (D-H)

Diffie-Hellman Key Exchange Protocol (D-H) is a cryptographic protocol [6] that allows two parties to establish together a common secret key over an insecure communication channel. After agreement on a common key, it can be used to encrypt messages in communications using a symmetric key technique. It generates a secret key common to both the sender and the receiver; this algorithm itself does not encrypt data. Although they never agreed on using a particular key, through mathematically linked processes the two parties can independently generate the same secret key and then use it to build a session key for use in asymmetric algorithm. This procedure is called *key agreement*, meaning that the two parties are agreeing on a key to use.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. We can define the discrete logarithm in the following way. Primitive Root: A primitive root of a prime number P as one whose powers modulo P generate all the integers from 1 to P-1 .That is, if "r" is a primitive root of the prime number P, then the numbers r mod P, r^2 mod P,….., rp^{-1} mod P are distinct and consist of the integers from 1 through P-1 in some permutation. For any integer b and a primitive root r of prime number P, we can find a unique exponent i such that $b= r^i$ (mod P) where $0 <= i <= (P - 1)$. The exponent i is referred to as the discrete logarithm of b for the base r, mod P. We express this value as $dlog_{r, P}$ (b).

The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key. Generation of secret is done in this way that first of all both users select their private and create public key. Then both users share their public key to each other and calculate the secret key, that having the same value in both side.

A. Algorithm of Diffie-Hellman Key Exchange Protocol:-

i. Let's there is a prime number "p" and an integer "r", here "r" is the primitive root of p.

ii. There are two users A and B. both select their X_A and X_B private value respectively.

iii. Compute the public values for both user using the formula-

$Y_A = (r)^{XA}$ MOD p and $Y_B = (r)^{XB}$ MOD p

iv. User A sends Y_A to user B, and user B sends Y_B to user A.

v. User A computes the key K as-

$K = (Y_B)^{XA}$ MOD p

vi. User B computes key K as-

$K = (Y_A)^{XB}$ MOD p

From these both, the value of key K will come same.

vii. Value of K will come in this way for user A

$K = (Y_B)^{XA}$ MOD p

$= ((r)^{XB}$ MOD p$)^{XA}$ MOD p

Value of K will come in this way for user B-

$K = (Y_A)^{XB}$ MOD p

$= ((r)^{XA}$MOD p$)^{XB}$ MOD p

$= (r^{XA})^{XB}$ MOD p

Fig.1 Diffie-Hellman algorithm

B. Diffie-Hellman diagram:-

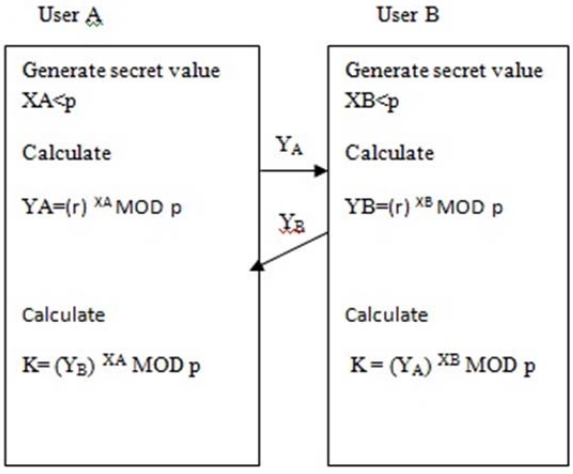

Fig. 2 Diffie – Hellman Key Exchange

C. Example of Diffie-Hellman Key Exchange protocol :-

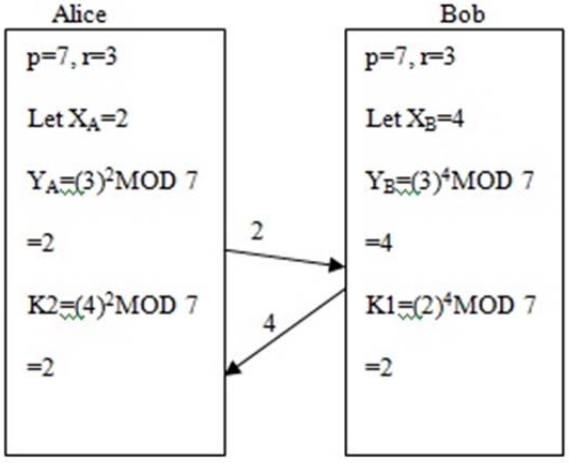

Fig. 3 Example of Diffie – Hellman Key Exchange

In this example K1=2 equal to K2=2, this type Alice and Bob agrees upon a common secret key and use this key for encryption and decryption of message in the communication.

IV. MAN-IN-MIDDLE ATTACK

The Man-in-Middle attack is the main problem with Diffie-Hellman key exchange [10]. In this attack, Ave intercepts Alice's public component and sends his own public component to Bob. When Bob transmits his public key, Ave interrupts and substitutes the value with his own public key and then sends it to Alice. Now Alice and Bob share a common secret key with Ave instead of each other. The algorithm of Man-in-Middle Attack is presented in fig. 4

A. Algorithm for Man-in-Middle Attack:-

i Ave prepares for the attack by generating two random private keys X_{M1} and X_{M2} & computes the public values Y_{M1} and Y_{M2}.
$Y_{M1}= (r)^{XM1}$ MOD p.
$Y_{M2}=(r)^{XM2}$ MOD p.

ii Alice transmits Y_A to Bob.

iii Ave intercepts Y_A and transmits Y_{M1} to Bob.

iv Bob transmits Y_B to Alice.

v Ave again intercepts Y_B and transmits Y_{M2} to Alice.

vi Bob receives Y_{M1}.

vii Alice receives Y_{M2}.

viii Alice computes K1= $(Y_{M2})^{XA}$ MOD p.

ix Bob computes key K2= $(Y_{M1})^{XB}$ MOD p.

x Ave computes key K1= $(Y_A)^{YM2}$ MOD p.
K2= $(Y_B)^{YM1}$ MOD p.

Fig. 4 Man-in-Middle Attack

Alice and Bob have different keys. But Ave has two keys one is similar to Alice's key and second is similar to Bob's key. Now Alice and Bob thinks that they share the secret key but in real Alice and Ave will share key K1 and Ave and Bob will share key K2. When Alice sends message to Bob, it is done in following ways:-

- Alice sends encrypted message.
- Ave intercepts that message, decrypt it by using keys because it has both keys, similar to Alice's and Bob's key.
- Ave reads that message, can send to Bob as it is or modify it.
- Bob receives message, thinks that it was sent by Alice but unfortunately it was sent by Ave.

This problem lies because Diffie-Hellman key exchange does not provide any authentication to the participants.

B. Example of Man-in-Middle Attack:-

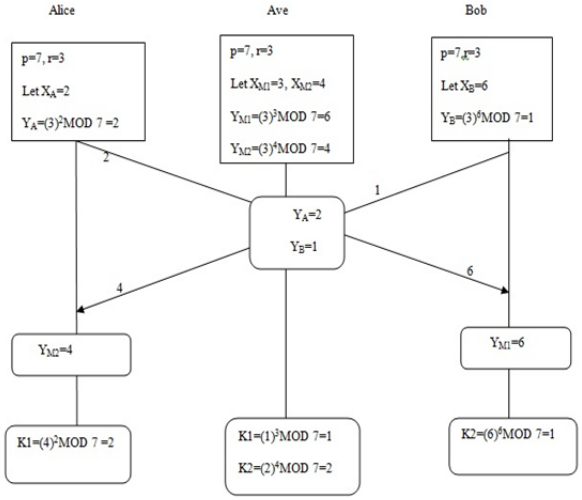

Fig.5 Man-in-Middle Attack

V. N-PARTY MAN-IN-MIDDLE ATTACK

It is not necessary there is always one middle man; there may be many attackers between sender and receiver. When client sends his public component to server, first attacker intercept it and sends own generated first public components to server and second to client but if there is another attacker then that first component intercepted by second attacker. In this type all attackers intercept public components of their neighbor users and generate their own keys which are similar to neighbor users and decrypt the messages.

A. N party Man-in-Middle Attack block diagram:-

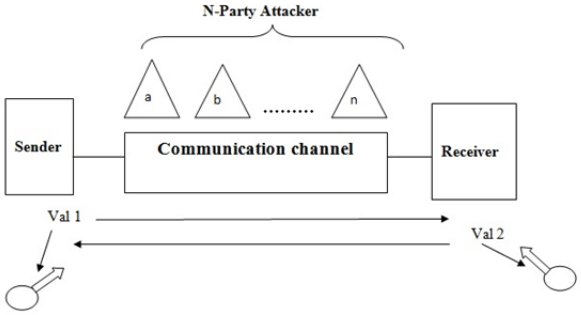

Fig. 6 N party Man-in-Middle Attack

B. Generation of N party Man-in-Middle Attack :-

Alice wants to communicate with Bob, so to generate a secret key between them; he sends his own public component to Bob. But there are many attackers between Alice and Bob. This whole process is performed in following way:-

- Alice generates own private key X_A and computes public component $Y_A=(r)^{XA} MOD\ P$.
- Bob generates own private key X_B and computes public component $Y_B=(r)^{XB} MOD\ P$.
- This type all attackers also generate their private keys and then compute public components.
- Suppose first attacker M1 generate private keys:- X_{MA1} and X_{MA2} and compute his public components:- $Y_{MA1}=(r)^{XMA1} MOD\ P$ $Y_{MA2}=(r)^{XMA2} MOD\ P$.
- Second attacker M2 generate private keys:- X_{MB1} and X_{MB2} and compute his public components:- $Y_{MB1}=(r)^{XMB1} MOD\ P$ $Y_{MB2}=(r)^{XMB2} MOD\ P$.
- In this way all attackers generate their private keys and then compute public components.
- When Alice sends his public component Y_A to Bob, M1 intercepts Y_A and sends own generated first public component (Y_{MA1}) to Bob and second(Y_{MA2}) to Alice.
- Alice receives Y_{MA2} and thinks that this is the Bob's public component and compute key ($K1=(Y_{MA2})^{XA} MOD\ P$).
- When middle man M1 sends his public component to Bob, there may be another attacker M2.
- M2 intercepts public component sent by M1 and sends own generated first public component (Y_{MB1}) to Bob and second (Y_{MB2}) to M1. He thinks M1 is the client, he does not know about any attacker.
- M1 computes his both keys:- $K1=(Y_{MB2})^{XMA1} MOD\ P$ and $K2=(Y_A)^{XMA2} MOD\ P$, one is similar to Alice and second is similar to M2. M1 communicate with Alice and M2 and Alice thinks that he is communicating with Bob.
- In this way all attackers compute their Keys. Last attacker MN sends his public component (Y_{MN1})to Bob and (Y_{MN2}) to attacker MM, and computes Keys $K1=(Y_B)^{XMN1} MOD\ P$ and $K2=(Y_{MM1})^{XMN2} MOD\ P$. one is similar to attacker MM and other with Bob.
- Bob receives public component (Y_{MN1}) from MN but thinks this is from Alice and computes own key $K2==(Y_{MN1})^{XB} MOD\ P$. Here Bob communicates with MN attacker not Alice. But he doesn't know about this.
- This type we can generate N number of attackers in Diffie-Hellman algorithm.

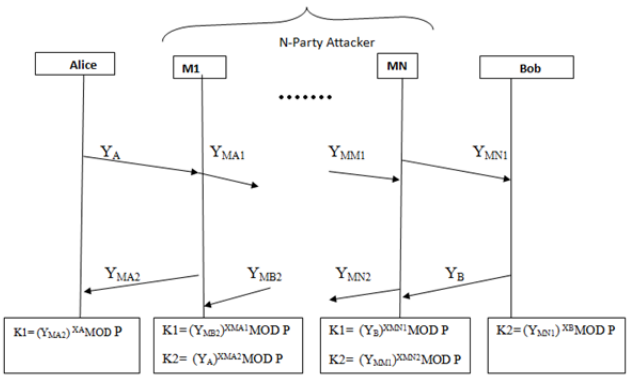

Fig. 7 N party Man-in-Middle Attack generation

VI. CONCLUSION

The Diffie-Hellman key exchange protocol is very effective scheme to generate a common secret key for both the sender and the receiver. It is easily susceptible to man in the middle attack. It cannot be used to encrypt the message and there is also a lack of authentication. But by mixing with RSA[10], Digital Signature [2] and other protocol variants, this problem improved by adding modulus operation on the private key [16]. That increases the entropy and decrease the autocorrelation. The Diffie - Hellman algorithm is enhanced by adding some more security codes or changes in the current algorithm [14]. We can extend it up to N attackers as men in the middle.

REFERENCES

[1]. Lein Harn, Manish Mehta and Wen-Jung Hsin "Integrating Diffie–Hellman Key Exchange into the Digital Signature Algorithm (DSA)", IEEE communications letters, vol. 8, no. 3, march 2004.

[2]. Raphael C.-W. Phan, Member," Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol ", IEEE communications letters, vol. 9, no. 6, June 2005.

[3]. Ik Rae Jeong, Jeong Ok Kwon, and Dong Hoon Lee ", Strong Diffie-Hellman-DSA Key Exchange", IEEE communications letters, vol. 11, no. 5, may 2007.

[4]. Nan Li," Research on Diffie-Hellman Key Exchange Protocol", 2nd International Conference on Computer Engineering and Technology, Vol 5, 2010.

[5]. Barun Biswas, Krishnendu Basuli, " A novel process for key exchange avoiding man-in-middle attack" International Journal of Advancements in Research & Technology, Volume 1, Issue 4, September-2012.

[6]. Barun Biswas, Krishnendu Basuli, Samar Sen Sarma," On a key exchange technique, avoiding Man in the-middle Attack", Journal of Global Research in Computer Science Volume 3, No. 9, +September 2012.

[7]. C. Krishna Kumar1, G. Jai Arul Jose1, C. Sajeev1 and C. Suyambulingom2", "Safety measures against Man-in-Middle Attack in Key-Exchange", ARPN Journal of Engineering and Applied Sciences, vol. 7, no. 2, February 2012.

[8]. Shilpi Gupta and Jaya Sharma," A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", 2012 IEEE International Conference on Computational Intelligence and Computing Research.

[9]. Mahmood Khalel Ibrahe," Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof", International Conference on Future Communication Networks, 2012.

[10]. Sunita, Neeraj Goyat , Annu Malik ,"Review of Diffie–Hellman key Exchange", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013.

[11]. Jagmohan Tanti1 and R Thangadurai,"Distribution of residues and primitive roots ", Proc. Indian Acad. Sci. (Math. Sci.) Vol. 123, No. 2, May 2013, pp. 203–211._c Indian Academy of Sciences.

[12]. Shahab Mirzadeh, Haitham Cruickshank, Member, IEEE, and Rahim Tafazolli, Senior Member, IEEE, "Secure Device Pairing" A survey IEEE communications surveys & tutorials, vol. 16, no. 1, first quarter 2014.

[13]. Shyam Deshmukh, Prof.Rahul Patil," Hybrid cryptography technique using modified Diffie-Hellman and RSA", International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014, 7302-7304.

[14]. Akta lamba, Lalit Garg,"Enhanced Diffie Hellman Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014.

[15]. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography, IEEE Transaction on Information Theory, 22(6), 644–654 .

[16]. Rohini, Er.Meenakshi Sharma,"Enhancing the Diffie- Hellman Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014.