Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Diffie Hellman Algorithm

Ekta Lamba
Research Scholar M.Tech
YIET, Gadholi,YamunaNagar, India

Lalit Garg
Associate Professor in CSE Department
YIET,Gadholi, YamunaNagar, India

Abstract*— *Diffie Hellman algorithm is an asymmetric cryptography scheme for the encryption and decrption of data over computer network. The algorithm allows two usrers to exchange a symmetric secret key through an insecure wired or wireless channel without any prior secrets. Crptography schemes are used in order to provide security to data against hacking and unauthorized access. One major problem with Diffie Hellman algorithm is the man-in-the-middle attack. The main aim of this paper is to study and analyse various enhancement schemes in the basic Diffie-Hellman algorithm.

Keywords*— *Diffie Hellman, wireless networks , crptography , asymmetric, encryption, decrption etc.

I. INTRODUCTION

By the last decade hacking and unauthorized access has been increased at very significant rate, by this threats many experts tends to provide solutions for these problems. Data encryption refers to mathematical calculations and algorithmic schemes that transform plaintext into cyphertext, a text that can't be read by unauthorized people. The recipient of an encrypted message uses a key which convert the ciphertext to plaintext. Security means freedom from the danger that no one can affect the integrity and confidentiality of the data.

The use of encryption/decryption is as old as the art of communication. In wartime, a ciphertext, can be used so that the opponent cannot get the transmission data. Simple ciphers include the substitution of letters in place of numbers, the spinning of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More sophisticated ciphers work according to sophisticated computer algorithms that rearranges the data bits in digital signals.

In order to get the contents of an encrypted signal, the correct decryption key is used. The key is an algorithm that reverses the work of the encryption algorithm. It becomes more difficult to attack on the communication without access to the key if the encryption algorithm is more sophisticated.

A). Diffie Hellman Algorithm

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography and is generally referred to as Diffie-Hellman key exchange. This key exachange technique is used in a number of commercial products. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

Diffie Hellman (DH) allows two users to exchange a symmetric secret key through an insecure wired or wireless channel and without any prior secrets[1].

Secure transmission is generally realised by encryption and authentication mechanisms; encryption protects all the data during transmission while authentication guarantees procedures to install permitted devices.[4]

Modifing the security of DH means improving the security of the protocols that use DH. DH works under the domain of integer Zn where n = p. P and a are the two parameters of DH where p is a large prime number and a is a generator selected from the cyclic group Zn. Two principals A and B can use the DH algorithm to exchange a symmetric key. The principal A chooses a private value a, then it chooses a large random prime P and a generator a. The public key of A is (p,a, a') and the private key is a. A sends its public key to B. After receiving A's public key, B chooses its own private key b and computes its public key (p,a, ab). B sends its public key to A. Now A and B computes their symmetric key [1].

Figure 1 shows a simple protocol that makes use of the Diffie-Hellman calculation and exchange. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key *XA*, calculate *YA*, and send that to user B. User B responds by generating a private value *XB* calculating *YB*, and sending *YB* to user A. Both users can now calculate the key. The necessary public values *q* and α would need to be known ahead of time. Alternatively, user A could pick values for *q* and α and include those in the first message[8]

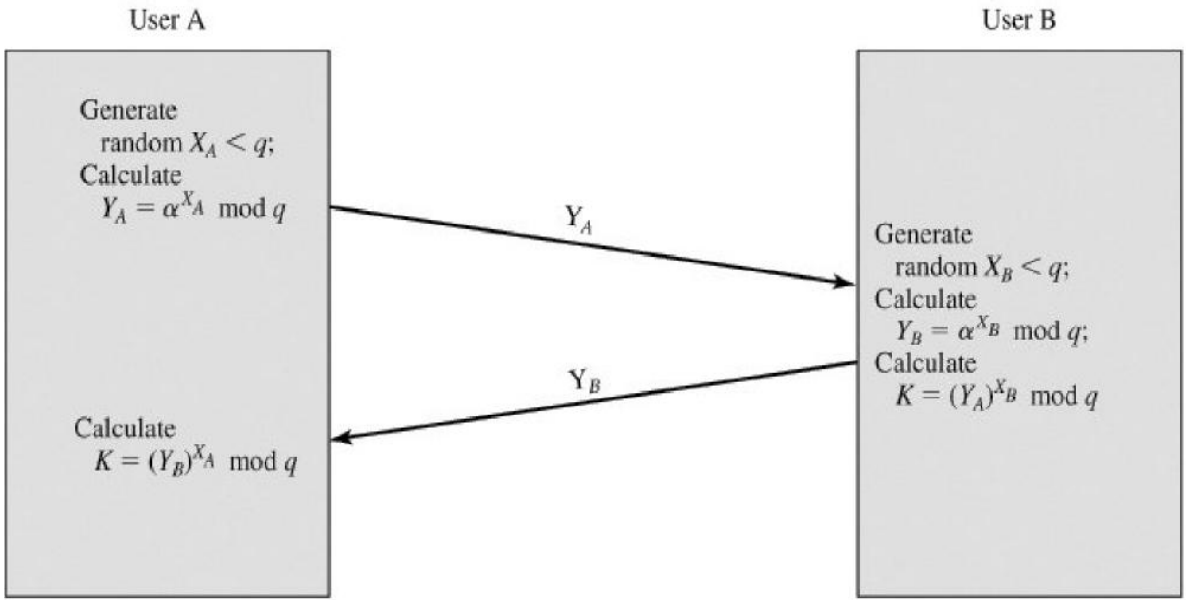

Figure 1. Diffie Hellman Algorithm

The protocol depicted in Figure 1.1 is insecure against a man-in-the-middle attack. The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.[8]

B). Vulnerabilities, Risks and Threats

Safe passage of Data is the prime issue for network for different types of services and it demands huge resources in security and encryption techniques. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher that is, the harder it is for unauthorized people to break it the better in general. However, as the strength of encryption/decryption increases, so does the cost. In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

II. **LITERATURE REVIEW**

In [1], P. Bhattacharya,in 2005,the author proposed two modifications of DH. The first modification is to change the domain to integer with n=2pt where Zn is still cyclic and the second modification is to change the domain to Gaussian arithmetic Z [i].

In [2], Ik Rae Jeong,in may 2007, provided an overview that to provide authentication to the Diffie-Hellman key exchange, a few integrated key exchange schemes which provide authentication using the DSA signature have been proposed. It pointed out that all of the previous Diffie-Hellman-DSA schemes do not provide security against session state reveal attacks. It also suggest a strong Diffie-Hellman-DSA scheme providing security against session state reveal attacks as well as forward secrecy and key independence.

In [4], Salvatore Cavalieri in 2009, deals with the problem of making secure data transmission inside Home and Building Automation environment; here, data exchanged may regard commands to actuators and/or private and secret information. The paper deals with this problem taking into account the KNX communication system, which at this moment, doesn't foresee any encryption and authentication mechanisms. A solution for data encryption and authentication will be presented and assessed, comparing it with the current state of the art.

In [5] , Eun-Jun Yoon, in 2009, proposed an efficient Diffie-Hellman-MAC key exchange scheme providing security against session state reveal attacks as well as forward secrecy and key independence.

In [7], S. Anahita Mortazavi, in 2011,in this author proposed an efficient many-to-many group key management protocol in distributed group communication. In this protocol, group members are managed in the hierarchical manner

logically. Two kinds of keys are used, asymmetric and symmetric keys. The leaf nodes in the key tree are the asymmetric keys of the corresponding group members and all the intermediate node keys are symmetric keys assigned to each intermediate node. For asymmetric key, Diffie-Hellman key agreement is introduced. To calculate intermediate node keys, members use codes assigned to each intermediate node key tree. Group members calculate intermediate node keys rather than distributed by a sponsor member. The features of this approach are that, no keys are exchanged between existing members at join, and only one key, the group key, is delivered to remaining members at leave.

In [8], Vishal Garg, in 2012, provided harder encryption with enhanced public key encryption protocol for security and proposed work can be implemented into any network to provide better security. It enhanced the hardness in security by improving the Diffie-Hellman encryption algorithm by adding some more security codes in current algorithm.

III. COMPARISION OF EXISTING TECHNIQES

Table 1 : Comparison between Classical and Gaussian DH

Algorithm	Key Size (in bits)	Time needed to compute secret key (in msec)
Classical DH	12	20
Gaussian DH	28	40

The above table is showing that the time needed to compute secret key in Gaussian DH is greater than the Classical DH.

IV. CONCLUSION

In order to provide more security to Diffie Hellman algorithm, different approaches have been followed till date. One is the mechanism of group keys in which only the group members know the secret key. Another approach is the one in which the key size has been increased. The comparison between the two DH methods was done according to the key size generated, which shows that the generated key size from the modified method is greater than the classical one. Attacking the methods shows that the time needed to compute the private key for the modified algorithm is greater than the classical one.Therefore, the modified method is more secure as more time is needed to crack the key. The more recent approach used is the inclusion of a mathematical function to make the key harder and the time required to crack the key here is even more than previous approaches , therefore is more secure.

REFERENCES

[1] P. Bhattacharya, M. Debbabi and H. Otrok, "Improving the Diffie-Heliman Secure Key Exchange", International Conference on Wireless Networks, Communications and Mobile Computing in 2005.

[2] 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.

[3] Zhen Cheng, Yufang Huang, Jin Xu,"Algorithm for Elliptic Curve Diffie-Hellman Key Exchange Based on DNA Tile Self-assembly",in 2008.

[4] Salvatore Cavalieri and Giovanni Cutuli," Implementing Encryption and Authentication in KNX using Diffie-Hellman and AES Algorithms",in 2009.

[5] Eun-Jun Yoon, Kee-Young Yoo," An Efficient Diffie-Hellman-MAC Key Exchange Scheme,"Fourth International Conference on Innovative Computing, Information and control, in 2009.

[6] Dongfang Zhang," A New Authentication and Key Agreement Protocol of 3G based on Diffie-Hellman Algorithm,"in 2010.

[7] S. Anahita Mortazavi, Alireza Nemaney Pour," An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSA", International symposium on computer networks and distributed systems, February 23-24, 2011.

[8] Vishal Garg, Rishu,"Improved Diffie-Hellman Algorithm for Network Security Enhancement", Int.J.Computer Technology & Applications,Vol 3 (4), 1327-1331 IJCTA | July-August 2012 Available online@www.ijcta.com 1327

[9] Emmanuel Bresson, Olivier Chevassut, David Pointcheva and Jean-Jacques Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange", in *Proc. Of ACM CCS '01,* ACM Press 2001.

[10] Michel Abdalla, Mihir Bellare, and Phillip Rogaway, " DHIES: An encryption scheme based on the Diffie-Hellman Problem", In Proc.of ACM CCS '01, ACM Press September18,2001.

[11] Jonathan C.Herzog, "The Diffie-Hellman Key-Agreement Scheme in the Strand-Space Model", 16th IEEE Computer Security Foundations Workshop (CSFW'03), 1063-6900/03 ,2003.

[12] 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

[13] Mario Cagaljm, Srdjan Capkun and Jean-Pierre Hubaux, "Key agreement in peer-to-peer wireless networks", Laboratory for Computer Communications and Applications (LCA) Ecole Polytechnique F´ed´erale de Lausanne

(EPFL), CH-1015 Lausanne Networked & Embedded Systems Laboratory (NESL), University of California, Los Angeles (UCLA), November 2004.

[14] Raphael C.-W. Phan, "Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol" , IEEE COMMUNICATIONS LETTERS, VOL. 9, NO. 6, JUNE 2005.

[15] L. Harn, W.-J. Hsin and M. Mehta, "Authenticated Diffie–Hellman key agreement protocol using a single cryptographic assumption", IEEE Proc.-Commun., Vol. 152, No. 4, August 2005.

