A Secure Wireless Communication Protocol using Diffie - Hellman Key Exchange

Atul Chaturvedi
PSIT, Kanpur, India

Neelam Srivastava
IET, Lucknow, India

Varun Shukla
PSIT, Kanpur, India

ABSTRACT
In 1976, Diffie and Hellman in their path breaking paper [5] proposed a two party key agreement protocol based on finite field. Diffie – Hellman Key Exchange Protocol [DH protocol] has unique importance in two party wireless communication scenarios. After this protocol several protocols have been proposed which were based on DH protocol but the Man in the middle attack raises a serious security concern on this protocol. Researchers have been working to overcome this security concern to design a new protocol. This paper proposes an authenticated key agreement protocol which is secure against Man in the middle attack. The authors also prove security issues of this protocol.

Keywords
Diffie – Hellman key agreement, Wireless Communication, Authenticated Key Agreement, Man in the Middle Attack (MITM), Security

1. INTRODUCTION
In modern communication scenario the security between two parties is vital. Here it is important to mention that, in a specific communication situation, the sender *Alice* and receiver *Bob* want to share the key using symmetric cryptography in the presence of an insecure channel. Insecure channel means presence of an adversary or hacker or intruder *Eve* [11].

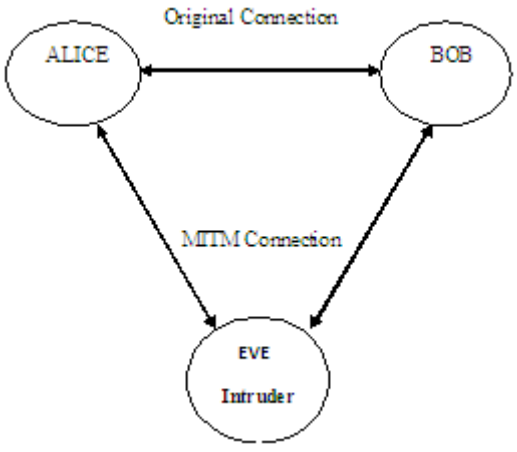

Figure 1: Showing the presence of intruder in MITM

Let us discuss the potential strength of an intruder in a communication environment. In many communication scenarios, for example in the financial transactions or in the financial industry, if the intruder can obtain sender's financial details such as bank statement, it will know that sender can have a large amount of money. This could imply that the potential reward of having access to sender's record exceeds the cost of launching many attacks on different protocol runs. The intruder is therefore highly motivated to attack the authentication stage of online transactions carried out between sender and bank [12].

In addition of the above mentioned situation, sometimes, the intruder attack is very dangerous say at the National or International security level. It's known that authentication, confidentiality, integrity and non-repudiation are the major cryptographic goals. In a military environment, a successful intruder attack is extremely dangerous. If non- repudiation fails, the presence of intruder can deny or change war timings, information related to number of soldiers which is a hazard for national security [14].

The adversary is capable enough to monitor the entire communication, thus depriving the integrity of a wireless communication. Diffie-Hellman in the path breaking paper [5] suggested some points to overcome this serious problem.

The rest of this paper organizes as follows. In section 2 we will discuss Diffie – Hellman Key agreement protocol and we discuss how the man in the middle attach deprives the integrity of communication. In section 3, we discuss the framework of an authenticated key agreement protocol and at last in section 4 we propose our authenticated key agreement protocol followed by its security consideration. The authors summarize this paper by conclusion and future scope.

2. RELATED WORK

2.1 Diffie – Hellman Key Agreement Protocol (DH Protocol):
The authors need to focus on hard problems which are the backbone of security of these DH-type protocols. Let *g* denote a generator of a group Z_p^*, where *p* is large prime which is good enough for security. Let *a* and *b* be randomly chosen elements in this group. With this frame one has to define some hard problems in Z_p^*.

Problem 1: [(*The Computational DH Problem (CDHP)*]: Given an generator g and the values of $g^a$and g^b in Z_p^*, compute the value of g^{ab} . For appropriate parameters, it is computational intractable to solve CDH problem.

Problem 2: [*The Discrete Logarithm Problem (DLP)*]: Given an generator *g* and the value of g^ain Z_p^*, compute the value of *a*.

The CDH problem is the foundation stone of DH - type protocol. The CDHP is breakable if one knows the how to crack DLP. We know that the most efficient means known to solve the CDHP is to solve the DLP and there is a strong

heuristic argument showing that DLP and CDHP are very likely to be equivalent [9, 13].

Now there is a discussion on basic DH protocol [5]. The sender *Alice* and receiver *Bob* has to agree on *p* which is a large prime and a non zero integer $modulo\ p$. Here the sender and receiver uses *p* and *g* publicly. It is assumed well that the communicating parties select *g* in such a way so that its order in Z_p^* is a large prime. Moving one step further, in order to maintain the integrity of wireless communication, even in the presence of adversary *Eve*, the sender selects a random integer, say '*a*' and kept it private. Similarly, on the other side, the receiver select a random integer say '*b*' and does the same. The sender *Alice* and receiver *Bob* by using this privately chosen integer compute $K_A = g^a mod\ p$ and $K_B = g^b mod\ p$ respectively. After the computation is over, they wish to exchange these calculated values. Since the communication channel is insecure, the adversary or hacker *Eve* can observe these computed values not random integers *a* and *b*. In continuation of this, now *Alice* and *Bob* both computes $K_{AB} \equiv (g^b)^a mod\ p$ and $K_{BA} \equiv (g^a)^b mod\ p$ respectively. Now they both have a common secret key $K = K_{AB} = K_{BA} = g^{ab} modp$ and in the insecure channel the adversary has limited ingredients to work on and the exchanged keys (or secret keys) remains safe which in turn enhancing the integrity and trust of wireless communication. After the invention of the DH protocol, most of the public key exchange protocols appear to be DH -type protocols [8].

Now as the aspect of Diffie-Hellman's work, one can say that calculating the value of $g^{ab} mod\ p$ from known exchanged values of $g^a mod\ p$ and $g^b mod\ p$ is the ultimate key exchange problem. These key exchange problems are very efficient in authenticated key exchange protocols that take the special constraints of wireless networks and mobile devices, such as limitations in bandwidth, computational power, memory space, usage of battery etc [6].

2.2 Man in the Middle Attack: It's time to discuss the man in the middle attack often abbreviated to MITM. It is an attack where the attacker or intruder or hacker, say *Eve* secretary relays and possibly alters the ongoing wireless communication between sender *Alice* and receiver *Bob* who believe they are directly communicating with each other. MITM can be a type of cyber attack when a malicious actor inserts itself into a conversation between sender and receiver, impersonates both parties and gains access to information that are two communicating parties are exactly trying to send to each other. SSL/TLS is overcoming this problem but recent research work [4] shows that attacks are possible even in SSL/TLS security [15, 16]. So there is a strict essence of developing a key exchange mechanism which has intense power of resisting MITM as an inbuilt feature because of the mathematics involved. It works as follows:

- *Alice* sends g^a to *Bob*.
- *Eve* can intercept g^a and pick random 'c' and generate g^c and send it to *Bob*.
- *Bob* will think that it is coming from *Alice* and *Bob*'s reply g^b is for *Alic*e but it goes to *Eve*.
- Again in the similar fashion, the *Eve* intercepts g^b, keep it with itself and send g^c to *Alice*.
- By this mechanism, intruder hacked the ongoing communication and made g^{ac} between sender and himself. Similarly, intruder calculates g^{bc} between it and receiver and hacked the ongoing communication.

Now intruder is in commanding position and can destroy cryptographic goals.

3. AUTHENTICATED KEY AGREEMENT PROTOCOL (AKAP)

In a key agreement protocol two or more distributed entities need to share some key in secret, called session key. This secret key can then be used to create a confidential communication environment amongst the entities[1,2,3]. Since the path breaking work of Diffie-Hellman[5] in 1976, several key agreement protocols have been proposed over the years [7,9,10,17]. A number of desirable attributes of such key agreement protocols have been identified. In today's modern world, most of the protocols are analyzed with such attributes. These are listed as under:

* **Known-key security**. Each run of a key agreement protocol between two entities *A* and *B* should produce a unique secret key which is independent of previous session keys, if any. Thus a protocol should still achieve its goal even if an adversary has learned some other session keys.

*** Perfect forward secrecy**. If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities should not be affected.

*** Key-compromise impersonation**. Suppose A's long-term private key is disclosed to an adversary he/she can impersonate A, since it is precisely this value that identifies A. This attribute requires that this loss should not enable such an adversary to impersonate other entities to A.

*** Unknown key-share**. It should not be possible to coerce A to share a key with entity B without A's knowledge, i.e., when A believes the key is shared with some entity C $\neq$ B, and B correctly believes the key is shared with A.

Key control. Neither entity should be able to force the session key to a preselected value.

4. THE PROPOSED SCHEME

4.1 Initial Setup: Two parties say *A*(lice) and *B*(ob) first agree on a large prime number *p* and an element *g* $(2 \leq g \leq p-2)$ which is a generator of the multiplicative group Z_p^*. These values are publicly known everyone present in communication scenario including *E* (ve).

- *A* randomly chooses her long term secret key *a* $(2 \leq a \leq p-2)$ and computes her long term public key $X_A = g^a$.

- *B* randomly chooses his long term secret key *b* $(2 \le b \le p-2)$ and computes her long term public key $X_b = g^b$.
- Thus, (a, X_A), and (b, X_B) are secret and public value pairs of *A* and *B* respectively.

Key Agreement: Here the authors describe the AKAP following the above notions. The protocol works in the following steps:

- A randomly chooses an integer *c*, computes $K_A = (X_B)^a$ and $Y_A = (K_A)^c$.
- A sends $h(Y_A)$ to *B*.
- Upon receiving Y_A, *B* randomly chooses an integer d, computes $K_B = (X_A)^b$ and $Y_B = (K_B)^d$.
- *B* sends $h(Y_b)$ to *A*.
- *B* also computes the shared key, $KEY_B = (Y_A)^d$.
- Upon receiving Y_B, *A* also computes $KEY_A = (Y_B)^c$.

4.2. Security Consideration: Here the authors have shown that the protocol meets the following desirable attributes under the assumption that the DL problem is hard.

- *Known-Key Security:* If *A* and *B* execute the regular protocol run, they clearly share their unique session key *K*, because

$$KEY_A = (Y_B)^c = \left((K_B)^d\right)^c = (K_B)^{cd}$$
$$= \left((X_A)^b\right)^{cd} = (X_A)^{bcd} = \left(g^a\right)^{bcd} = (g)^{abcd}$$
$$= \left(g^b\right)^{acd} = (X_B)^{acd} = \left((X_B)^a\right)^{cd} = (K_A)^{cd}$$
$$= \left((K_A)^c\right)^d = (Y_A)^d = KEY_B$$

- *(Perfect) Forward Secrecy***:** During the computation of the session key *K* for each entity, the random integers c, d still act on it. An adversary who captured their private keys a or b should extract K_a or K_b from the information Y_a and Y_b to know the previous or next session keys between them. However, this is the hard discrete logarithm problem . Hence, under the assumption that the DLP in Z_p^* is computationally infeasible, AKAP meets the *forward secrecy* requirement.
- *Key-Compromise Impersonation***:** Suppose *A*'s long-term private key, *a*, is disclosed. Now an adversary who knows this value can clearly impersonate *A*. Is it possible for the adversary impersonates *B* to *A* without knowing the *B*'s long-term private key, *b*? For the success of the impersonation, the adversary must know *A*'s ephemeral key *c* at least. So, also in this case, the adversary should extract *c* from *A*'s ephemeral public value $Y_A = (K_A)^c = \left(g^{ab}\right)^c$. This also contradicts that DLP is hard in Z_p^*.
- *Unknown Key-share***:** It is important examine the unknown key-share attack that allows an adversary *E* to make one party believe *K* to be shared with *E* while it is in fact shared with a different party. A common scenario is that *E* has X_A certified without knowing the private key *c* of *A*, and uses it to talk with *B* as *E* while she poses as *B* to *A* simultaneously. Our protocol is secure against this attack because for *E*, we have $h(Y_A)$ in computing each *K*
- *Key Control:* As the same argument in the above, the key-control is clearly impossible for the third party. The only possibility of *key-control* attack may be brought out by the participant of the protocol, *B*. But for the entity *B*, to make the party, *A* generate the session key KEY_B which is pre-selected value by *B*, for example *B* should solve the following $(Y_A)^d$. But this again falls into the DLP.

5. CONCLUSION AND FUTURE SCOPE

On the basis of above discussion the authors can conclude that MITM is always hazardous for secure wireless communication. This protocol is strong enough to resist MITM which is a very unique feature. The authors kept their discussion limited to two parties communicating over a channel which is said to be insecure because of the presence of an intruder but the concept proposed can be utilized for group key agreement protocols also. Since the protocol is MITM resist, it can be implemented in various two party transaction schemes or group communication like military ad-hoc networks or in mobile communication protocols.

6. REFERENCES

[1] Bellare, M., and Rogaway, P. Entity authentication and key distribution. In Advances in Cryptology – CRYPTO ' 93 (1994), D. R. Stinson, Ed., vol. 773 of Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany

[2] Bellare, M., Canetti, R., and Krawczyk, H. Modular approach to the design and analysis of key exchange protocols. In Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC-98) (New York, May 23–26 1998), ACM Press, pp. 419–428.

[3] Blake-Wilson, S., and Menezes, A., Authenticated Diffie-Hellman key agreement protocols. In Fifth Annual Workshop on Selected Areas in Cryptography (SAC '98) (1999), Lecture Notes in Computer Science, Springer Verlag, pp. 339– 361.

[4] Burkholder P., SSL-Man in the middle attack, February 2002,v 2.0, www.sans.org/reading-room/

[5] Diffie W., & Hellman M., *New directions in cryptography*, IEEE Trans. Inform. Theory,22(6),1976,644-654.

[6] Hoeper, K. and Gong, G. : Efficient Key Exchange Protocols for Wireless Networks and Mobile Devices, Technical Report, CARR 2005

[7] Law L.,,A.Menezes, M.Qu, J.Solinas, S.Vanstone, *An efficient Protocol for Authenticated Key Agreement*, Technical Report CORR98-05,Department of CO, University of Waterloo,1998

[8] Law L., Menezes A. , Qu M., Solinas J., & Vanstone S., *An efficient protocol for authenticated key agreement*, Design,Codes and Cryptography, 28(2), 2003, 119-134.

[9] Maurer U., S. Wolf, The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithm, SIAM Journal of Computing 28 (5) (1999) 1689–1721.].

[10] Menezes A., M.Qu, & S.Vanstone, *Key agreement and the need for authentication*, Proceedings of PKS'95, Toranto,Canada,1995

[11] Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. Handbook of applied cryptography. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431- 9868, USA, 1997.

[12] Nguyen, L. H., Rational authentication protocols, http://eprint.iacr.org/ 2011/070.pdf, 2011

[13] Oorschot, V., and Wiener, M. J. On Diffie-Hellman key agreement with short exponents. In Advances in Cryptology – EUROCRYPT ' 96 (1996), U. Maurer, Ed., Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany, pp. 332–343.

[14] Şen, S., John A., Clark, Juan E. Tapiador, Security Threats in Mobile Ad Hoc Networks, Department of Computer Science, University of York, YO10 5DD, UK, pp.1-22.

[15] Vaudenay, S., Security flaws induced by CBC padding - applications to SSL, IPSEC, WTLS... In Advances in Cryptology – EUROCRYPT ' 02 (2002), Lecture Notes in Computer Science, Springer-Verlag, pp. 534–545.

[16] Wagner, D., and Schneier, B. Analysis of the SSL 3.0 protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, 1996. Also published in The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pp. 29–40.

[17] Wilson B., D.Johnson, A.Menezes, *Key agreement protocol and their security analysis*, Proceedings of Sixth IMA International Conference on Cryptography and Coding, Cirencester, UK, 1997, 30-45.