Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Various key exchange techniques in wireless networks: A review

Mohit Gambhir

Verispire Technologies Pvt. Ltd., Delhi, India
Email: mohitgambhir@gmail.com

ABSTRACT

Key exchange protocol is the public key cryptographic protocol where a platform is provided for sharing keys between two parties. In a key exchange protocol, private keys can also be exchanged among multiple receivers over a public insecure communication channels and agree upon a common session key and that session key will be used later to make a secure communication among parties. The main objective of key exchange protocol is that private keys of multiple parties are shared without thinking of their secrecy. Private keys are very confidential to be shared but here in this mechanism this is allowed. In this paper a comparison study is done on various key exchange mechanisms and brings up their strengths and shortcomings.

KEYWORDS: Key exchange protocol, Secure communication, Private key, Wireless networks

***Corresponding author:**

Mohit Gambhir

Verispire Technologies Pvt. Ltd., Delhi, India

Email: mohitgambhir@gmail.com

INTRODUCTION

There are several techniques which have been proposed for the exchanging of public keys. This is a challenge to exchange cryptographic keys securely. Key exchange protocol is one of the public key cryptographic primitives that provides a platform to negotiate keys among a group of parties. The only goal of the key exchange protocol is that group of parties can share the private keys without compromising their secrecy. For Key exchange dilemma, the Diffie-Hellman key exchange protocol was the first practical solution. In Diffie-Hellman protocol, two parties are allowed to exchange a secret key over unsecured channels and they are unknown to each other. In this paper, a comparison study among various existing key exchange techniques is done.

Organisation of the paper is as follows: section 2 explains various techniques used for key exchange; section 3 shows comparison among these techniques along with advantages and disadvantages; section 4 concludes the paper.

Methods and Material

Lot of research have been done on key exchange protocol like:

- In Najmus Saqib's scheme[1], Elliptic Curve Cryptography has been used to improve the existing key exchange algorithm. This paper provides an efficient and improved implementation of key exchange which is based on Elliptic Curve Cryptography (ECC). In this protocol, Alice and Bob selects two random numbers and performs some scaler multiplications. This computation needs the private key of Alice and public key of Bob. This method is used to prevent Man-in-the-middle-attack in key exchange. To intercept the key, Eve must know the private key to generate inverse of the private key. So this method tries to prevent MITM attack. But the problem here is that in ECDH there is no authentication and the attack is not fully prevented. Elliptic Curve Diffie Hellman (ECDH) is suitable for limited sensor nodes, if there are multiple nodes in the communication then this method experiences Man- in- the-middle- attack.
- In Ankit Taparia, Saroj Kumar Panigrahy and Sanjay Kumar Jena's scheme[2], the key exchange is done securely using the method of string comparison. In this protocol, the commitment scheme is used. This commitment scheme allows a user to choose a value which is unseen to other users and later the value would be disclosed. This enhanced Diffie Hellman key exchange uses three phases- Initialization, Exchange and verification. In initialization phase, A and B selects k-bit random string and prepares a message to exchange. In their message 0 and 1 are used to prevent reflection attack. Then the commitment value is exchanged with the message in Exchange phase and checks whether the commitment value is correct or not. After this the verification phase is done.

Both users generate verification strings if they are matched then both accepts the DH parameters. In this protocol, there is an issue that a user has to commit on a value i.e. on a message before seeing the others message.

- In Aqeel Sahi Khader, David Lai's scheme[3], the secure Diffie Hellman is achieved by using binary sequences in passwords. The passwords are chosen and converted them in binary numbers. This technique is for shorter length. For longer sequences, the Geffe Generator is used. Geffe generator is a pseudo random sequence generator. This is chosen for some reasons like it has superior complexity and best features for example it has balanced distribution of 0's and 1's in its output. Geffe generator uses three registers to generate one random sequence. When the binary sequence is generated, then three kinds of statistical test are used to check whether the randomness of sequence is good or not. In this each sequence is checked with three tests i.e. frequency test, serial test, poker test again and again. If any of the test is failed, the sequence is failed so this is very lengthy process and time consuming.
- In Young-Seok Lee's scheme[4], this paper is proposed for key exchange in satellite environment. This paper suggested a protocol which identifies the attack without the data sharing between NCC & RCST by introducing timestamp and overcome the disadvantages of existing protocols. In this, the fixed public value is not used rather it uses fresh values. It uses Diffie Hellman key exchange to share keys between NCC (Network control centre) and RCST (Return Channel Satellite Terminal). Here the timestamp is created and prevented man in middle attack between NCC & Satellite and between RCST & Satellite. This is thirteen step procedure to check whether man in middle attack is true or not. The arithmetic calculations are used in timestamp created and in it the ids of users are also used so that replay attacks can be prevented. This approach is helpful in identifying the attack before sharing the data between NCC and RCST. And also it takes less computation time.
- In Barun Biswas, Krishnendu Basuli's scheme[5], A novel key exchange process is suggested for prevention of man in middle attack. This paper defines the cryptography and its types, Man in middle attack in Diffiehellman and its algorithm to prevent MITM. The algorithm suggests to use e as a secret number as the base of log. So both users use e in computing their public keys and exchange with each other. Then both users calculates a secret key with their public keys and cross verify the keys. If the number calculated is prime then the keys are not attacked. Here the protocol uses e because if the key is attacked then only key value will be changed. There might not be the e value as base of log and the man in middle attack can be prevented. But here is an issue that the base value can be same as the users selected and then the data is attacked.

- In M.S. Durairajan, Dr. R. Saravanan's scheme[6], The fingerprint technique is used and explained. To prevent the data to be hacked by middle man biometric technique is introduced. As biometric fingerprints are very secure to safely store the data. In this the private key is replaced by value of fingerprints. The fingerprints are first converted into a cancellable template and then the binary values are calculated. That binary values then converted into decimal forms and that decimal number becomes the private key to be shared. This technique is used to share keys between sender and receiver with full authentication. Here the key exchange algorithm used is Diffie Hellman. The users' fingerprints are stored in database and they needed only at the time of authentication. If fingerprints are matched in database, then both users can communicate and are authenticated. But in this technique, there is an issue that it is also not fully secured. Fingerprints can also be hacked through many ways e.g from a glass in bar. If password is hacked, it can be changed but if fingerprint is hacked it cannot change.
- In Nissa Mehibel, M'hamed Hamadouche's scheme[7], the elliptic curves are used for the encryption and decryption. The protocol used for securing and authenticating the key exchange is proposed in this research. Here two parties that want to communicate with each other agree on using Elliptic curve Ep (a,b), p is a prime number and a generator of G. Alice and Bob chooses a random number on elliptic curve and calculate their public keys using arithmetic formulae respectively. Thus the elliptic curves are utilised here for the key exchange to be preventive from middle man. In this protocol there are less number of operations performed than previous approaches.
- In Eun-Jun Yoon, Il-SooJeon's scheme[8], A secured and efficient Diffie Hellman key agreement protocol is suggested using Chebyshev chaotic map. Chebyshev chaotic map is very popular technique and several researches have been done in this area. In this approach the author tried to reduce the computational cost and no need of timestamp here. There is third party between Alice and Bob which is reliable and act as Kdc. Third party say here, Trent shared the different secret key with Alice and Bob. Here a message authentication code, MAC by Alice and Bob is generated using collision resistant secured hash function, it is one-way hash function. If the MACA and MACB values are equal,then both the users are authenticated and communication would be done. This protocol is resistant to MITM attack, replay attack also. But in this approach the third party reliability cannot be trusted as this is only an assumption.

COMPARISON STUDY OF EXISTING TECHNIQUES

Table 1 shows comparison among various techniques discussed in the previous section along with its advantages and disadvantages.

CONCLUSION

In this paper various key exchange techniques proposed by various researchers is defined along with their advantage and disadvantages. Comparisons among
existing techniques help researchers to identify problems in current solution which further motivate them to provide solution also.

Table 1: Comparison of various Key Exchange Protocol techniques

S.No.	Author	Methodology	Advantage	Disadvantage
1.	NajmusSaqib[1]	ECDH technique	Eve cannot know the private key for generation of inverse of private key.	Applicable to limited sensor nodes only and for large no. of nodes it can experience MITM attack.
2.	AnkitTapariav[2]	String Comparison	Faster Execution Less computational time and low overhead.	Users have to commit on a value or a message without knowing the other's message.
3.	David Lai [3]	Using binary sequence and Geffe Generator(checked from 3 tests)	Superior complexity. Balanced distribution of 0 and 1 in its output.	Any of test failure causes a halt, so it is a lengthy process and time consuming.
4.	Young Seok Lee [4]	Timestamp created	Identify attack before sharing the data. Less computation time.	Not used for the real environment but in satellite environment.
5.	BarunBiswas[5]	Using e as base of the secret key.	Key can be attacked but not necessarily the base e.	Cannot sure for the secure authentication. e might be same used by the user.
6.	M.S. Durairajan[6]	Biometric Fingerprint	Secure to store data.	Fingerprints can be stolen and cannot be changed for further communication.
7.	Eun-Jun Yoon[7]	Chebyshev chaotic map	No timestamp required for communication. Message authentication code is generated for authentication.	No reliability of third party.

REFERENCES

1. NajmusSaqib, Key Exchange Protocol for WSN Resilient against Man in the Middle Attack, Advances in Computer Applications (ICACA), IEEE International Conference, 2016; 265-269
2. AnkitTaparia, Saroj Kumar Panigrahy and Sanjay Kumar Jena, Secure Key Exchange Using Enhanced Diffie-Hellman Protocol Based on String Comparison, Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference, 2017; 722-726

3. AqeelSahiKhader, David Lai, Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol, Telecommunications (ICT), 22nd International Conference, 2015; 204-208
4. Young-Seok Lee, Improvement of Key Exchange Protocol to prevent Man-in-the-middle Attack in the Satellite Environment published in Ubiquitous and Future Networks (ICUFN), Eighth IEEE International Conference, 2016; 408-413
5. Barun Biswas, Krishnendu Basuli, Anovel process for key exchange avoiding man-in-middle attack, Int. Journal Adv. Research & Technology: 2012; 1(4): 1-5
6. M. S. Durairajan, Dr.R. Saravanan, Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism, Int. Journal Chem Tech Research Coden (USA): IJCRGG. 2014; 6(9): 4359-4365
7. Nissa Mehibel, M'hamed Hamadouche, A New Approach of Elliptic Curve Diffie-Hellman Key Exchange, 5th International Conference on Electrical Engineering – Boumerdes (ICEE-B), 2017; 1-6
8. Eun-Jun Yoon, Il-Soo Jeon, An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map, Commun Nonlinear Sci Numer Simulat. 2011; 16(6): 2383 – 2389