A novel Diffie Hellman protocol based on NIST p 192 Curve for securing internet of Things

Manu Banga, Ph.D Scholar, ASET, Amity University, Noida
Dr. Abhay Bansal, Professor, ASET, Amity University, Noida
Dr. Pritam Gajkumar Shah, Professor, Jain University, Bangalore

Abstract-
Internet of Things suffers from limited bandwidth, energy sources as well as computational power. Most of the IoT devices works on battery and can not afford the luxury of traditional public key cryptography. The traditional DH protocol puts lot of pressure on resource constrained architecture of IoT. This paper proposes a novel Diffie Hellman protocol based on elliptical curve NIST p-192 curves for optimizing these resources. The novelty of DH protocol based on elliptical curve demonstrated through MIRACL crypto library and programming is done by using C.

Key Terms: Diffie Hellman protocol, Elliptical curve cryptography etc.

Introduction-

The principle behind method used for facilitating exchanging key on a secure basis but rational Diffie-Hellman Algorithm has certain deficiency lack of secure information in cloud sharing [3,6] for overcoming these shortcomings and pitfalls a hybrid algorithm based on Elliptic curve is proposed[8,9], making a hybrid of Elliptic Curve Cryptography and Diffie-Hellman for optimizing resources by using less space.

Related Work:

In encryption of key value during exchange $q\ prime\ number$[7,5] is used and α primitive root of prime number at a cost of hit encompass a noteworthy contact as attacker established admission of user systems private data. Furthermore attacker gained access of Administrator Rights [12,13] may damage by inflicting virus over key value and can lead to failure so authentication over key exchange is a subject of great concern [9,12,13] of present condition of Denial to Service attacks

Diffie-Hellman Key Exchange Algorithm

Global Public Element:

$$q\ prime\ number\ \alpha < q\ and\ \alpha\ is\ a\ primitive\ root\ of\ q$$

Assuming

User A Key Generation:

Select private $X_A, X_A < q$

Calculate public

$$Y_A, Y_A = \alpha^{XA} mod\ q$$

User A Key Generation:

Select private $X_A, X_A < q$

Calculate public

$$Y_B, Y_B = \alpha^{XB} mod\ q$$

Calculation of Secret Key by User A:

$$K = \left({Y_B}^{XA}\right) mod\ q$$

Calculation of Secret Key by User B:

$$K = \left({Y_A}^{XB}\right) mod\ q$$

Figure 1: Diffie-Hellman Key Exchange Algorithm

Diffie Hellman Approach Used for securing information:

Let message send from sender to receiver using secure channel be spitted into a bits of strams as q

q="1553155263514823959911559963512318072201696448283789374332238389722325183519588380870733218456247565501469452460037901080459403831947734394960519170198923701023413789901139595618958910197168732905128154347241575884606136382020170206727560910672233361943949107653098308760662464801566174921641400954277735473 19"

Selecting prime value α = 3

A Private key a calculation

1190524734126777733565106951973477053802465284426

A Public key a calculation

1249625390796473492344207477469034892363377243767227081494386257510536341450409250086055906487212762791420916968893197782683012749487344446036896292370681499639442252837451433058328949990637053397933804440282973439379421170124223687337362273294097900735869638483022884392328402272366644315570930157152476423 02

B Private key Calculation

2306756492730380738467841721333949128292433584 21

B Public key Calculation

1406694966073587830866186708484052153568952687993485185224918547899132817619992294087830024445945004338377499188973754671915753237401710613945431671460876924069865587369635709735153402164989943433167171114272076555779201773142106899408723984898298283923513771702166986380606086678740506233029081736666903484 93

A Session Key=

7657596014433267498922881207640812898706461353040069373180316788006951235735912995159096547698472094113334421561759503653871359569785737246061497803856418565359178872806211696844802911164769583227750250409794497708222246030013138461784479817680883656951181180214887501320783863773549917328094402587043666116 8

B Session Key=

7657596014433267498922881207640812898706461353040069373180316788006951235735912995159096547698472094113334421561759503653871359569785737246061497803856418565359178872806211696844802911164769583227750250409794497708222246030013138461784479817680883656951181180214887501320783863773549917328094402587043666116 8

A and B keys are the same

Figure 2:-Diffie-Hellman Key exchange without using Elliptic Curves

Approach Used:

Elliptic-curve Diffie–Hellman: Being an unidentified enter contract set of rules with the purpose of allowing party, every have an unrestricted–confidential type, in the direction of creating a joint undisclosed above an unselfconfident way.[1][2][3] The joint undisclosed might subsist straightly define key value, also could create another solution further encrypting succeeding exchanges by means of a symmetric type ciphering. Hybrid Algorithm Diffie–Hellman protocol on ECC by managing key sharing between parties in Internet of Things framework and thereby authenticate the message over channel between sender and receiver for managing resource allocation on sensors, grid. The novel protocol on depending on certificate exchange so we have achieved secure medium on sharing of information in Internet of Things. Thus, less prone to unauthorized access by attacker so using 198-bit Elliptic Curve Cryptography.

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000003

The base point G in compressed form is:

G = 03 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D

and in uncompressed form is:

G = 04 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D
9B2F2F6D 9C5628A7 844163D0 15BE8634 4082AA88 D95E2F9D

Finally the order n of G and the cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFE 26F2FC17 0F69466A 74DEFD8D

h = 01

Using Hybrid Elliptic Curves Diffie-Hellman Key

A key estimate value

B key estimate value=

735723040707006201325038495845927737553053854578654864324

B computed value=

735723040707006201325038495845927737553053854578654864324

A and B computed exactly equal value but with less space corresponding to A key derived with our novel approach

Results:

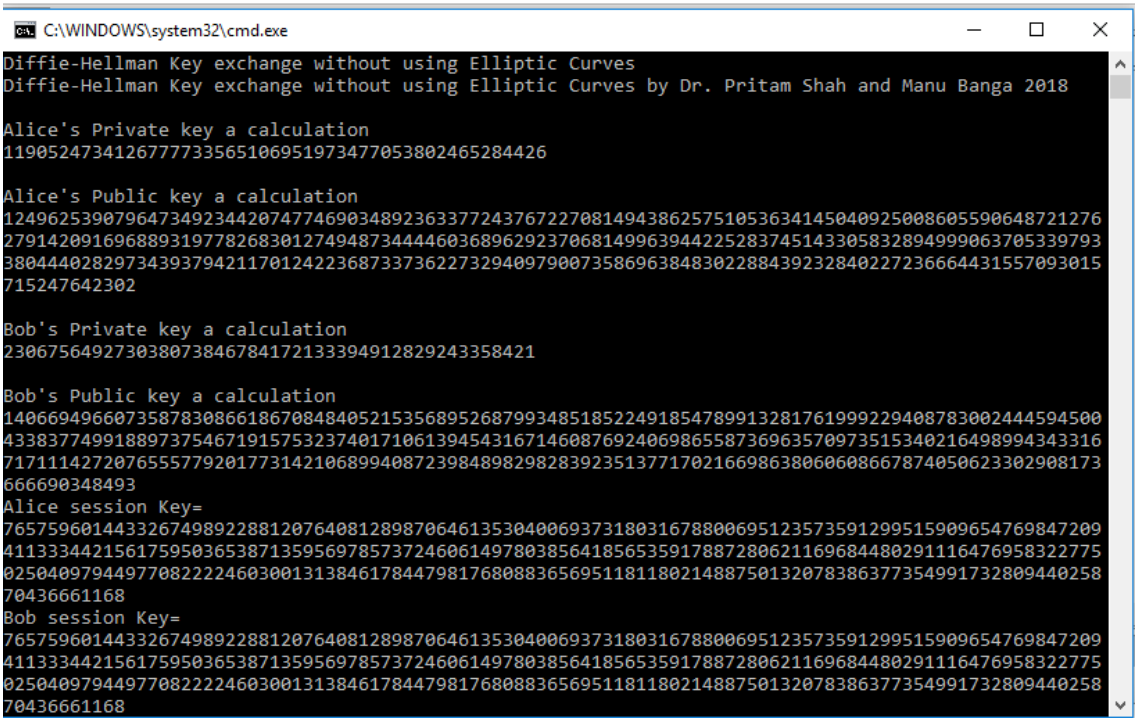

Figure3: Screenshot of Diffie-Hellman Key exchange with using Elliptic Curves by Dr. Pritam Shah and Manu Banga 2018

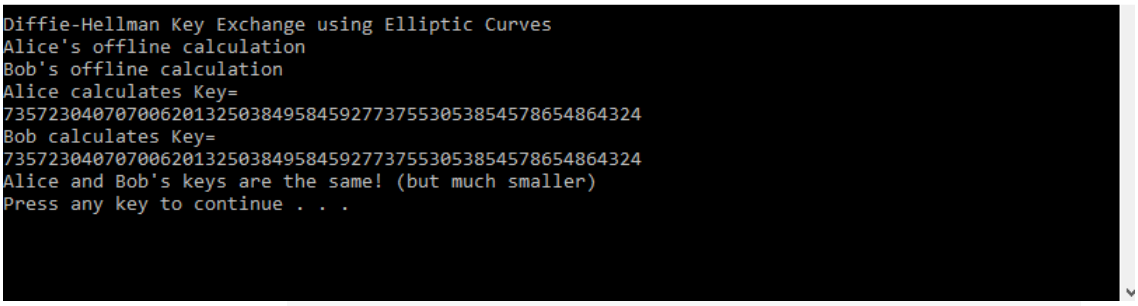

Figure 4: Screenshot of comparing key values Diffie-Hellman Key exchange with using Elliptic Curves by Dr. Pritam Shah and Manu Banga 2018

Conclusion:

By this hybrid approach, resources are utilized optimally, thereby will save the bandwidth as well as storage requirements reducing overhead as key size reduced, due to quadratic nature elliptical equation will have solution, one bit storage thus reducing space and time overheads

References:

1. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.
2. Bala, D. Q., Maity, S., & Jena, S. K. (2017, May). Mutual authentication for IoT smart environment using certificate-less public key cryptography. In Sensing, Signal Processing and Security (ICSSS), 2017 Third International Conference on (pp. 29-34). IEEE.
3. Bhattasali, T., Chaki, R., & Chaki, N. (2013, December). Secure and trusted cloud of things. In India Conference (INDICON), 2013 Annual IEEE (pp. 1-6). IEEE.

4. Martín-Fernández, F., Caballero-Gil, P., & Caballero-Gil, C. (2016). Authentication based on non-interactive zero-knowledge proofs for the internet of things. Sensors, 16(1), 75.
5. Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. IEEE Access, 5, 19293-19304.
6. Simplicio Jr, M. A., Silva, M. V., Alves, R. C., & Shibata, T. K. (2017). Lightweight and escrow-less authenticated key agreement for the internet of things. Computer Communications, 98, 43-51.
7. Win, E. K., Yoshihisa, T., Ishi, Y., Kawakami, T., Teranishi, Y., & Shimojo, S. (2017, July). A Lightweight Multi-receiver Encryption Scheme with Mutual Authentication. In Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual (Vol. 2, pp. 491-497). IEEE.
8. Taha, S., & Shen, X. (2013). ALPP: anonymous and location privacy preserving scheme for mobile IPv6 heterogeneous networks. Security and Communication Networks, 6(4), 401-419.
9. Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems, 89, 110-125.
10. Wazid, M., Das, A. K., & Lee, J. H. (2018). Authentication protocols for the internet of drones: taxonomy, analysis and future directions. Journal of Ambient Intelligence and Humanized Computing, 1-10.
11. Qiu, Y., & Ma, M. (2015). Security Issues and Approaches in M2M Communications. In Securing Cyber-Physical Systems (pp. 276-295). CRC Press.
12. Bala, D. Q., Maity, S., & Jena, S. K. (2017, February). A lightweight remote user authentication protocol for smart E-health networking environment. In I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on (pp. 10-15). IEEE.
13. Jamshiya, P. K., & Menon, D. M. (2018, April). Design of a Trusted Third Party Key Exchange Protocol for Secure Internet of Things (IoT). In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 1834-1838). IEEE.
14. Robot, W. M. S. NO PAPER ID TITLE AND AUTHOR'S NAME PAGE NO. Analysis, 1, 2017_004.
15. Karantaidou, I., Halkidis, S. T., Petridou, S., Mamatas, L., & Stephanides, G. (2018, June). Pairing-Based Cryptography on the Internet of Things: A Feasibility Study. In International Conference on Wired/Wireless Internet Communication (pp. 219-230). Springer, Cham.