GROUP KEY APPLICATIONS IN BLUETOOTH PICONET

Sachin Dev Kanawat*

Pankaj Singh Parihar**

Apurva Pandey***

Anurag Maloo***

Abhishek Singh****

ABSTRACT

Bluetooth is a wireless technology, where Bluetooth devices are connected in ad-hoc fashion to form a piconet. Through the analysis of the piconet group key generation based on authenticated Deffie-Hellman group key generation protocol [1], each device in the Bluetooth piconet requires large memory space to store the keys. Although the protocol serves good security features, the number of messages exchange and total number of round is more so it requires high computing capability of each unit. The protocol has high overhead to compute the group key when a new member joins or leave into or from the group, it leads computational and communicational cost. In the present work Dynamic GKE(Group Key Exchange) protocol is more suitable to generate group key for Bluetooth piconet than GDH.2 and ECGDH protocols. Deffie-Hellman based Dynamic GKE (Group Key Exchange) protocol [47] has comparatively low round as well as communication cost for group key generation then existing one. The Dynamic GKE protocol is non-authenticated one, so before applying this we assume each mobile client (slave) and the powerful node(master) is already been authenticated manually or some other Deffie-Hellman based method have been used to authenticate the devices. The Dynamic GKE protocol is applicable for piconet group key generation. Dynamic GKE protocol is more efficient in the case of member join/leave operations and secure for piconet group key generation

***Keywords**: Dynamic GKE (Group Key Exchange), Authenticated, Non-authenticated, Piconet, Master/Slave, Diffie-Hellman key exchange key.*

*Department of Computer Engineering, Institute of Technology & Management, Rajasthan.

**Assistant Professor, Department of Computer Engineering, Institute of Technology & Management, Rajasthan.

***Lecturer, Department of Computer Engineering, Institute of Technology & Management, Rajasthan.

****Department of Computer Engineering, Institute of Technology & Management, Rajasthan, India.

I. INTRODUCTION

Bluetooth was designed as a low-cost, low-power wireless networking technology to be used in Personal Area Networking (PAN). Bluetooth is one of the most promising and a highly emerging wireless technology that provides robustness, low power-consumption and low cost for short-range communication purpose. Bluetooth is the code name for an alliance between mobile communications and mobile computing companies to develop a short-range communications standard that allows wireless data communications among almost any device to another device within ranges of about 10 meters to 100 meters.

Considering Bluetooth piconet wireless network environments such as wireless local area networks and cellular mobile networks they may be regarded as asymmetric (imbalanced) wireless networks. An imbalanced wireless network consists of mobile clients and a powerful node. Generally, mobile clients may use some mobile devices (i.e., cellular phone or PDA) to access mobile applications through the powerful node. If such mobile clients want to perform a secure conference using their mobile devices through cellular mobile networks or wireless local area networks, they must establish a secure group key to encrypt/decrypt the transmitted messages. Considering the computing capability of mobile devices, a flexible approach is to shift the computational burden from the mobile devices to the powerful node. This approach reduces the computational costs on mobile nodes. Consequently, several group key agreement protocols for the imbalanced wireless network have been proposed.

Security requirements for Group Key Application protocol:

Forward secrecy: When a new member joins the group, he/she cannot compute the previous established group keys to decrypt the past encrypted messages.

Backward secrecy: When an old member leaves the group, he/she cannot compute the subsequent group keys to decrypt the future encrypted messages.

II. GKE PROTOCOL

A. Dynamic GKE protocol Overview

Since the recently proposed GKE (Group Key Exchange) protocols for wireless network environment sare non-authenticated ones. By its very nature, a non-authenticated group key exchange protocol cannot provide participant and message authentication, so it must rely on the authenticated network channel or use other schemes to provide authentication in advance. Since Bluetooth piconet is confronted with great threats such as eavesdropping, without user authentication. Here, as like the recently proposed GKE protocols, we assume that each mobile client and the powerful node have already authenticated mutually. Here, we focus on

the application possibilities of a non-authenticated GKE protocol in Bluetooth piconet for group key generation. In this paper, we propose a new group key exchange protocol with the dynamic property for wireless network environments. Under several security assumptions, we will prove that the proposed protocol is secure against passive attack and provides forward/backward secrecy for dynamic member joining/leaving. Meanwhile, we demonstrate that the proposed protocol also satisfies the contributiveness property. As compared with the existing Group Key Agreement protocol based on Authenticated Diffie-Hellman, our protocol provides better performance in terms of computational cost, round number and communication cost.

B. Deffie-Hellman based group key family protocol Protocol Overview

In 2003, Boyd and Nieto presented a one-round GKE protocol. Their protocol is efficient for imbalanced wireless networks, but it lacks forward secrecy. Bresson et al. proposed a two-round GKE protocol for imbalanced wireless networks. Unfortunately, their protocol provides only partial forward secrecy. This partial forward secrecy means that leaking the mobile nodes private keys do not reveal any information about the previous establishment group keys, but leaking the powerful node's private key will enable an adversary to reconstruct the previous group keys. Subsequently, Nam et al. also presented an improvement on the protocol proposed by Bressonet al. Elliptic Curve Cryptography (ECC) is a public key cryptosystem based on elliptic curves [48]. The attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. The Group Elliptic Curve Diffie-Hellman (GECDH) protocol is an extension of GDH based on ECDLP. GECDH can also be divided into two stages: upflow and downflow. The protocol has been proposed in 2006, it has required n number of round to calculate group key. In 2007, Tseng demonstrated that the Nam et al.'s protocol has a security weakness. In their protocol, the powerful node can pre-determine the group key. That is, Nam et al.'s protocol is not a contributory GKE protocol. For repairing this weakness, Tseng also proposed a secure group key exchange protocol for imbalanced wireless networks. However, Tseng's GKE protocol does not deal with dynamic member joining/leaving functionality. Note that the dynamic joining/leaving functionality means that other participants need not to re-run the protocol when a participant joins or leaves the group. For a GKE protocol, it is important to provide this dynamic functionality, especially for wireless network environments. For providing dynamic joining/leaving functionality, Chuang and Tseng recently proposed a dynamic group key exchange protocol for imbalanced wireless networks. However, their protocol requires three rounds to establish a group key.

III. GROUP KEY AGREEMENT PROTOCOL FOR WIRELESS AD-HOC NETWORK

Group Diffie-Hellman (GDH) is a class protocols presented by Steiner et al. GDH.2 and GDH.3 are two of them. These protocols are natural extensions of 2-party Diffie-Hellman key exchange to the n-party case. In 2-party case, each member selects its secret share and sends exponent of this secret share α^{Ni} to its peer. Both members can calculate the key α^{N_1N2} by using its own share. In n-party case, if a member Mi knows exponent of secret share of other members $\alpha^{N_1N2\cdots N_{i-1}N_{i+1}\cdots N_n}$, then using its own share, it can calculate group key as $\alpha^{N_1N2\cdots\cdots N_n}$.

Suppose Ni is the secret exponent of member Mi and α is a generator in the algebraic group. GDH.2 works as follows:

(1) Mi → Mi+1 : { $\alpha^{\frac{N_1\ldots N_i}{N_j}}$ | j ∈ [1,i] }, $\alpha^{N_1\ldots N_i}$ i ∈ [1, n-1]

(2) Mn → ALL Mi: { $\alpha^{\frac{N_1\ldots N_n}{N_j}}$ | j ∈ [1, n-1] }

Stage (1) consists of n-1 rounds. In every round i, Mi unicasts Mi+1 a collection of i values. Of these, i-1 items are intermediate, which are, $\alpha^{N_2N_3\ldots N_i}$, $\alpha^{N_1N_3\ldots N_i}$ … $\alpha^{N_1N2\ldots N_{i-1}}$, and one is cardinal, $\alpha^{N_1\ldots N_i}$. When upflow reaches Mn, Mn can calculate the group key as $\alpha^{N_1N_2\ldots N_n}$. Also, Mn calculates the intermediate values $\alpha^{N_2N_3\ldots N_n}$, $\alpha^{N_1N_3\ldots N_n}$ …, $\alpha^{N_2N_3\ldots N_{n-2}N_n}$. In stage (2), Mn broadcasts these n-1 intermediate values to all group members. When member Mi receives these broadcast intermediate, it can calculate the group key as $\alpha^{N1N_2\ldots N_n}$ by using its own share Ni to the corresponding intermediate. Figure1.1 shows GDH.2 with 4 members.

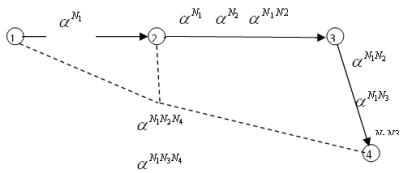

Figure 1.1 GDH.2 with n=4

To reduce the computational burden on Mi, GDH.3 protocol is provided. In the upflow stage of GDH.3, only one item, cardinal, instead of i items in GDH.2, is calculated and sent to the next member. Thus computation overload of i-1 intermediate items is reduced. GDH.3 consists of four stages.

(1) Mi → Mi+1: $\alpha^{\prod N_p | p\in[1,i]}$ i ∈ [1, n-2]

(2) Mn-1 → ALL : $\alpha^{\prod N_p | p \in [1,n-1]}$

(3) Mi → Mn : $\alpha^{\frac{\prod N_p | p \in [1,n-1]}{N_i}}$

(4) Mn → ALL : { $\alpha^{\frac{\prod N_p | p \in [1,n]}{N_i}}$ | i ∈ [1, n] }

First stage collects the exponentiation of every member up to Mn-1. After first stage is complete, Mn-1 obtains $\alpha^{\prod N_p | p \in [1,n-1]}$. In stage 2, Mn-1 broadcasts $\alpha^{\prod N_p | p \in [1,n-1]}$ to every member. In stage 3, every member factors out (divided by) its own exponent from $\alpha^{\prod N_p | p \in [1,n-1]}$ and sends the result to Mn. In stage 4, Mn raises every message received in stage 3 with its exponent and returns the result back to respective member. Thus every member can now calculate the Key as $\alpha^{\prod N_p | p \in [1,n]}$.

The problem of GDH.3 is that n-1 unicast messages are sent to Mn in stage 3, which may congest Mn.

Asokan and Ginzboorg provided a similar extension to GDH.2. In their method, all members share a password P. Each member Mi generates a secret share Si. The protocol works as follows:

Mi → Mi+1: $g^{s_1 s_2 \ldots s_i}$, i =1, .. n-2

Mn-1 → ALL: $g^{s_1 s_2 \ldots s_{n-1}}$

Mi → Mn: $\{g^{s_1 s_2 \ldots s_{n-1} \hat{s}_i / s_i}\}_P$

Mn → Mi : $\{g^{s_1 s_2 \ldots s_n \hat{s}_i / s_i}\}_P$

All above 4 stages are same as those in GDH.3, except stage 3. In stage 3, every member encrypts the revised intermediate key using share password P and sends it to Mn. In stage 4, instead of using multicast as in GDH.3, Mn unicasts the result to every member. It is suggested in the paper, the following step 5 may be used for verification. Some members broadcast the key message to make sure some other members decide the same key.

Mi → ALL: Mi, {Mi, H(M1,M2, .. , Mn)}K for some i

This method will provide good forward secrecy. However, it requires a shared password P. To get such a password is a problem itself.

IV. COMPONENTS IN SECURITY REQUIREMENTS

ECGDH (Elliptic Curve Based Group Deffie-Hellman) protocol is an efficient and secure group communication protocol based on ECDLP (Elliptic Curve Discrete Logarithm

Problem). The attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. However, the methods for computing general elliptic curve discrete logarithms are much less efficient than those for factoring or computing conventional discrete logarithms and it indicates that more computation time is required for ECC. GECDH canalso be divided into two stages: upflow and downflow. The upflow stage collects contributions from all group members. The downflow stage broadcasts the intermediate values to all group members for calculating the shared group key. To describe this in more detail, let ($M_1, M_2, \dots, M_n$) be a group of users, the i-th round of upflow stage is as follows:

M_i, where 0< i ≤ n receives a sequence of (i −1) intermediate key values { $(N_1 \dots N_{i-1})/N_k \; G | k \in [1, i-1]$ } and one cardinal value $K_{i-1} = N_1 \dots N_{i-1} G$.

M_i Generates its own contribution N_i .

M_i computes the new cardinal value $K_i = N_i K_{i-1}$.

The old cardinal value becomes one of the intermediate values.

Multiply each old intermediate value with N_i thus producing a set of new intermediate values.

If i<n, M_i sends K_i and the new intermediate values to M_{i+1} .

V. CONCLUSION

In this present work, we have proposed a new dynamic GKE protocol for Bluetooth piconet group key generation. Under the decision Diffie-Hellman (DDH), the computation Diffie-Hellman (CDH) and the hash function assumptions, the proposed protocol is secure against passive attacks and provides forward/backward secrecy for member joining/leaving. The number of message exchanged, round calculation, unicast messages and broadcast messages for group key generation is better than the previous [1] paper. The previous one was static while proposed one is dynamic in the case of group key generation when new members join/leave the group.

REFERENCES

1. Yu Xin, Wang ZhaoShun, Chu RongGong , "Application of Group Key Agreement Based on Authenticated Diffie-Hellman for Bluetooth Piconet," 2009 WASE International Conference on Information Engineering.
2. WHITFIELD DIFFIE AND MARTIN E. HELLMAN,"New Directions in Cryptography," EEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976.

3. Bluetooth SIG, "Specification of the Bluetooth System," Specification Volume 1, v1.0B, December 1, 1999.
4. J. Kardach. "Bluetooth architecture overview," Intel Technology Journal, (Q2):7, May 2000.
5. P. Johansson, M. Kazantzidis, R. Kapoor, M. Gerla, "Bluetooth: an Enabler for Personal Area Networking," IEEE Network, Vol. 15, No.5, Sept.- Oct. 2001, pp. 28-37.
6. Markus Jakobsson and Susanne Wetzel. "Security Weaknesses in Bluetooth," RSA Conference, 2001, pp. 176-191.
7. Lidong Zhou and Zygmunt J. Haas. "Securing Ad Hoc Networks," IEEE Network Magazine, November/ December 1999, 16(6):pp. 24-30.
8. Ludovic Rousseau, Christophe Arnoux, and Cedric Cardonnel, "A Trusted Device to Secure a Bluetooth Piconet," Published in Proc. of Gemplus Developer Conference, Paris, France, June 20-21, 2001.
9. Yuh-Shyan Chenand Tsung-Hung Lin, "A CENTRALIZED TIME-SLOT LEASING-BASED QOS ROUTING PROTOCOLOVER BLUETOOTH WPANS," 2005 IEEE conference.
10. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, "A Security Solution for IEEE802.11's Ad-hoc Mode: Password-Authentication and Group-Diffie-Hellman Key Exchange," International Journal of Wireless and Mobile Computing. Special Issue on Security of Computer Network and Mobile Systems. Volume2, Number1, pages4–13, Inder science, 2007.
11. Karen Scarfone, John Padgette, "Guide to Bluetooth Security," NIST Special Publication 800-121
12. Kahate, A 2003, "Cryptography and Network Security,"1st Edition TATA McGraw-Hill Company, India.
13. Subir Biswas, Syed Rehan Afzal, Jong-bin Koh, Mustafa Hasan, Gunhee Lee, and Dong-kyoo Kim , "An Enhanced Approach to Providing Secure Point-to-Multipoint Communication in Bluetooth Piconets," IEEE Network Magazine, 2007.
14. G Lamm, G Falauto, J Estrada, J Gadiyaram. "Bluetooth Wireless Networks Security Features." Proceedings of the IEEE Workshop on Information Assurance and Security, 2001.
15. Juha T. Vainio. "Bluetooth Security." Technical report, Dept. of Computer Science and Engineering, Helsinki University of Technology, 2000.

16. "The Official Bluetooth wireless information site", http://www.bluetooth.com/Bluetooth/learn/basics.
17. Rania Abdelhameed, Sabira Khatun, Borhanuddin Mohd Ali and Abdul Rahman Ramli , "Authentication Model Based Bluetooth enabled Mobile phone," Journal of Computer Science 1 (2):200-203,2005.
18. ZHIGUO WAN, "AUTHENTICATION AND KEY ESTABLISHMENT IN WIRELESS NETWORKS," NATIONAL UNIVERSITY OF SINGAPORE 2006.
19. I.Ingemarsson,D.T.Tang,andC.K.Wong,"Aconference key distribution system," IEEETrans.Inform.Theory,28(5):714-720,Sept.1982.
20. Ford Long Wong, "Protocols and technologies for security in pervasive computing and communications," Technical Report No.709, UCAM-CL-TR-709 ISSN1476-2986, January 2008.
21. Ford-Long Wong,Frank Stajano and Jolyon Clulow, "Repairing the Bluetooth pairing protocol," B.Christianson et al.(Eds.):Security Protocols 2005.
22. Chatschik Bisdikian, Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich , "An Overview of the Bluetooth Wireless Technology," IBM Research Report, Computer Science, RC 22109 (W0107-009) 6 June 2001.
23. MIN-SHIANG HWANG, CHENG-CHILEE, JI-ZHELEE, CHAO-CHEN YANG "A Secure Protocol for Bluetooth Piconets Using Elliptic Curve Cryptography," Springer Science+Business Media, Inc. Manufactured in The Netherlands, Telecommunication Systems 29:3,165–180, 2005.
24. Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Nctwork, 0890-8044/ 1999.
25. Karima MAALAOUI, Leila AZOUZ SAIDANE, "Priority Based Intra Piconet Scheduling Scheme for QoS Guaranties in Bluetooth Networks," 1EEE Network, 978-1-4244-4671-1/ 2009.
26. Roger I. Khazan, Robert A. Figueiredo, Ran Canetti, Cynthia D. McLain, Robert K. Cunningham, "SECURING COMMUNICATION OF DYNAMIC GROUPS IN DYNAMIC NETWORK-CENTRIC ENVIRONMENTS," United States Air Force under Air Force Contract FA8721-05-C-0002.
27. C. K. Wong, M. Gouda and S. Lam, Secure Group Communications Using Key Graphs, SIGCOMM 1998.

28. E. Fujisaki and T. Okamoto, Secure Integration of Asymmetric and Symmetric Encryption Schemes, Advances in Cryptology - CRYPTO 1999, Lecture Notes in Computer Science, Vol. 1666, 1999, pp. 537–554.
29. Chung-Hsin Liu, Yun-Mou Hou, "The study of the Bluetooth circular path," International Conference on Multi Media and Information Technology, 2008.
30. Chung-Hsin Liu, Sheng-Shiang Chang, Zhao-Cheng Ye, "The study for the optimal routing of Bluetooth Piconet," ICIS 2009, November 24-26, 2009.
31. Khaled Morsi , Xiong Huagang, Gao Qiang, "Performance Estimation and Evaluation of Bluetooth Frequency Hopping Selection Kernel," IEEE Networks, 2009.
32. M. J. Morón, R. Luque, and E. Casilari, "Modeling of the Transmission Delay in Bluetooth Piconets under Serial Port Profile," IEEE Transactions on Consumer Electronics, Vol. 56, No. 4, November 2010.
33. Daniele Miorandi, Carlo Caimi and Andrea Zanella, "Performance Characterization of a Bluetooth Piconet with Multi–Slot Packets," IEEE Networks, 2003.
34. Zhihua Tao, Zihua Guo, Richard Yao, "Piconet Security in IEEE 802.15.3 WPAN," IEEE Networks, 2005.
35. Bibo Jiang, Xiulin Hu, "A Survey of Group Key Management," International Conference on Computer Science and Software Engineering, 2008.
36. Mark Manulis, "Security-Focused Survey on Group Key Exchange Protocols," HGI Network and Data Security Group Technical Report 2006.
37. Chung Kei Wong, Mohamed Gouda, Simon s. Lam, "Secure Group Communications Using Key Graphs," National Science Foundation GRANT No. CDA-9624082,1999.
38. N. Asokan, Philip Ginzboorg, "Key Agreement In Ad-Hoc Networks," Preprint submitted to Elsevier Preprint, 2000.
39. Maarit Hietalahti, "Key Establishment in Ad-hoc Networks," Tik-110.501 Seminaron Network Security, HUTTML2000.
40. Scott C.-H.Huang, Frances Yaoa, Minming Li ,WeiliWu, "Lower bounds and new constructions on secure group communication schemes," PublishedbyElsevierB.V. 2008.
41. Jukka Kaavi, "Group Key Distribution in Ad-Hoc Networks Using MIKEY," HUTT-110.551Seminar on Internetworking, 2005.
42. Michael Steiner Gene Tsudik Michael Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication," 1996 ACM Press 0-89791-829-0196/03.

43. Klaus Becker, Uta Wine, "Communication Complexity of Group Key Distribution," t ACM Press 19981-581 134074/98/1 1.
44. Mukesh Singhal, Rendong Bai,Yun Lin,Yongwei Wang,Mengkun Yang, Qingyu Zhang,"Key Management Protocols for Wireless Networks," 2002.
45. Jelena Mi sic, Vojislav B. Mi sic,KaLok Chan, Talk and let talk: performance of Bluetooth piconets with synchronous traffic," 2003 Elsevier, AdHocNetworks3(2005)451–477.
46. Yuh-Shyan Chen and Tsung-Hung Lin, "A CENTRALIZED TIME-SLOT LEASING-BASED QOS ROUTING PROTOCOL OVER BLUETOOTH WPANS," IEEE Networks, 2005.
47. su-Yang Wu, Yuh-Min Tseng*, and Ching-Wen Yu, "Two-round contributory group key exchange protocol for wireless network environments," hindavi/journal/WCN, 2010.