www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-5, Issue-3, June-2015

International Journal of Engineering and Management Research

Page Number: 480-482

A Review of HB Family Security Protocol

Preeti[1], Sachin Kumar[2]

[1]M. Tech Student, Department of Electronics and Communication Engineering, MERI College of Engineering and Technology, Sampla, Rohtak, INDIA

[2]Assistant Professor, Department of Electronics and Communication Engineering, MERI College of Engineering and Technology, Sampla, Rohtak, INDIA

ABSTRACT

This paper presented a review on designing of HB++ protocol by using verilog. The literature review shows the related work on the lightweight authentication protocol and it also describe that authenticity is important for many applications such as in RFID systems and sensor networks[11] because the adversary can easily inject the message. The study shows that in 2001, Hopper and Blum proposed a HB protocol but this protocol works well against passive attack not well secure against active attack. In 2005 Juels and Weis proposed HB+ a new version of HB protocol. This protocol works well against active attack but it is not well secure against man-in-the-middle attack. In 2006, Bringer proposed HB++ protocol to secure against man-in-the-middle attack from adversaries in Gilbert(2005). It is called as HB++ protocol. On the countenance of literature review we describe the conclusion and future scope. The protocol which is at the forefront of current research effort is HB++ protocol which is a lightweight authentication protocol. HB++ protocol has been attracted significant attention and become promising protocol for RFID systems. The design is effective enough to be used in resource constrained pervasive devices like RFID.

***Keywords*-----** HB family, authentication protocol, learning parity with noise, security and privacy, protection, RFID

I. INTRODUCTION

HB++ is a light-weight authentication protocol given by Bringer, Chabanne and Dottox in 2006. It is a communication protocol which is designed with less complexity in order to reduce overhead in terms of more computations.The security of the protocol is based on conjectured hardness on the LPN (Learning parity with noise). The protocol is proved secure against MIMA(man-in-the-middle attack). It consists variousbitwise operations like AND, OR, XOR gates. The paper also describes that an HB++ protocol act as an authenticationprotocol forRFID technology because most of the RFID products lack security related functionality due to the hardware limitation of the low-cost RFID tags and satisfies integrity, forward secrecy and untraceability and provides stronger resistance to various attack such as tracing attacks, replay attacks etc.

It generally protects from man-in-the-middle-attack but MIMA(man-in-middle-attack) can succeed only when the attacker can be impersonate each end point to their satisfaction as expected from the legitimate other end. Today the systems of constrained devices are more common and their industrial/military importance is still growing. This paper presented a review on designing of HB++ protocol by using verilog to get secure communication. The protocol provides mutual authenticity and untraceability to protect the security and privacy of carriers. Compared to other protocol our protocol not only meets the fundamental requirements but is also lightweight enough to be implemented on RFID systems.

The paper is organized as follows: Section I describe introduction of HB++ protocol. Section II describes the literature review. Section III conclude the conclusion and Section IV describe the future scope.

II. LITERATURE REVIEW

In this section, related works on the lightweight authentication protocols are presented. A series of ultra lightweight protocols with bitwise operators and other simple function have been proposed for low-cost RFID systems.

Peris-copez et al. proposed LMPA [10], the protocol is efficient and requires less gates, which uses pseudonyms and various bitwise operation to realize tag anonymity and data integrity. However, it has been proved vulnerable to the full-disclosure and de-synchronization attack, in which an

attacker could interfere with both entities during the unit rounds to disclosure all sensitive secret key identifiers.

Chien's SASI [4] is a typical ultra-lightweight protocol in which public sub-messages are built via bitwise operation, Exclusive-OR (XOR) operation is the main functional component that is required, and pseudonym is pre-shared as the secret index to determine a matched record in a database. The de-synchronization attack can be resisted to the dynamic up data mechanism which is applied for storing the old key and the potential key to resist the de-synchronous attacks. Meanwhile, the use of addition mod 2^n is realistic for low-cost and low-power applications and this protocol cannot defend against the tracing attacks.

Furthermore, Phan [14] and Cuo et al. pointed out that SASI with limited integrity protection does not satisfy the desired objective of untraceable, and the protocol does not achieve the resistance to Dos and tracking attacks.

Hopper and Blum's HB protocol [6] is suitable for pervasive computing environment since it only requires scalar dot product operation of binary vectors. The security of these schemes rely on the hardness of the computational LPN problem while the HB protocol focuses on the major passive attacks a series of modified variants HB+, HB++ [9]have been improved to resist active attack, along with preserving HB's advantages of low requirements for tag resources to be exerted. The family of protocols is considered tobe secure against active attack, and can be exerted with so few resources.

Zhou et al. proposed a lightweight anti-design preserving authentication protocol [5], which is suitable for pervasive computing environments since only the capacity of hash function and XOR operation are required. In the protocol, the backend database keeps the former record of the random key up data to prevent the active attacks prevailing tags.

Chien and den proposed a mutual authentication scheme [7] on EPC global class 1 Gen 2 tag which uses CRC checksum code to detect error and verify the integrity of transmitted data. Meanwhile, access and kill command are used to detect cloned tags, withstand the malicious eavesdropping (monitor) readers, and a producer can implicitly keep track of tagged items. The updated unit key and access key are updated to enhance forward security. The random numbers are integrated to degrade the various attack such as tracing attack. Due to the linear properties of the RC function the protocol is proved vulnerable for the Dos attack [16,7]. Moreover, persistent certification by the brute security mode may increasingly burden the server and the overall performance will be reduced.

Kulseng et al.'s protocol in [9] is designed with mutual authentication to secure the transfer of RFID tags. The minimalistic cryptography such as physically functions and LFSR(Linear Feedback Shift Register) are used to realize the transfer. The protocol is efficient in hardware and practically suitable for low cost systems.

III. CONCLUSION

In this paper various security protocols and designing of HB family have been studied. The literature review shows that the HB++ protocolprovideboth tag-to-reader and reader-to-tag authentication and are resistant against common RFID attacks. The study shows that our design is efficient in terms of resources and so is suitable for use in constrained RFID systems. The protocol provides a reasonable amount of security in various systems. Compared to other protocols proposed in literature review, our HB++ protocol remain lightweight in terms of area and computation time, while still achieving the required security and privacy properties.

IV. FUTURESCOPE & CONCLUSION

A further suggestion for future investigation is to improve the security process or improve the compactness of the designing by using few gates,slices,flip-flops etc.It may be possible to design the perfect security protocol by using few gates, slices and flip flop. Future research directions in this field includes, above everything else, design ofa better low cost protocols. The protocols must provide enough security. Other NP-hard problems may be used to design such protocols. Another important factor is our design can be improved by pipelining the different functional stages.

REFERENCES

[1] C. M-chen, S-M.chehen, X.Zheng, L.Han, H.Wang and H,-M.S"Pitfalls in an ECC- based lightweight authentication protocol for low cost RFID,"Journal of Information Hiding and Multiple Signal Processing.", volume 5,no. 4,2014.

[2] T.Yeh, Y.Wang, T.Kuo and S.Way, "Securing RFID systems conforming to EPC class1 generation standard", Expert systems with Applications,volume. 37,no. 12,pp. 7678-7682,2010

[3] L. Kulseng, Y.Wei and Y.Guan, "Lightweight mutunal authentication and ownership transfer for RFID systems", 2010 Proc. IEEE INFOCOM, pp. 1-5,2010.

[4] T.Cao, E.Bertino and L.Hong,"Security Analysis of the SASI protocol," IEEE Transaction Dependable and secure computing, volume 6,no. 1,pp. 73-77,2009.

[5] S.Zhou,Z.Zhang, Z.Luo E.C Woy,"A lightweight antidesynchronization RFID authentication protocol", Information Systems Fronteirs, pp 1-8,2009.

[6] J.Bringer and M.Chabanne,"Trusted-HB:A low-cost version of HB srcecure against man-in-the-middle Attacks", IEEE Transaction on Information Theory , volume,54,No. 7,pp-4339-4342,2008.

[7] H.Y.Chien and CH cheu "Mutunal authentication protocol for RFID conforming to EPC class 1 gen. 2 standards", computer standards and Interfaces, volume 2. pp-254-259,2007.

[8] H.Y.Chien, "SASI: Anew ultra lightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Transactions on Dependable and secure computing, vol. 4.No. 4, pp. 337-340, 2007.
[9] J.Manilla and A.Peinade,"HB-MP:Afurther step in the HB-families of lightweight authentication protocols" computer networks,vol.5,No. 9,pp. 2262-2267,2007.
[10] P. Peris-Lopez, J.C. Hernandez- Casine J.M.E. Tapiador and A. Ribagorda "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags", Proc. Of the 2nd workshop on RFID security, Graz, Ausrric, 2006.
[11] Xiuli Ren and HaibinYa "Security mechanism for wireless sensor networks", IJCSNS, volume 6, No.3, March 2006.
[12] Julein Bringer, Herv'eChabanne, and Emmanuelle Dottax. "HB++: a lightweight authentication protocol secure against some attacks". In IEEE Computer Soceity Press, SecPerU 2006, Lyon, France, June 2006.
[13] G. Gilbert, M. Robshaw and H. Sibert, An active attack against HB+ -a probably secure lightweight authentication protocol, Cryptology ePrint Archive , Report 2005/237, 2005.
[14] R.C.W.Phanx,"Cryptanalysis of a new ultraweight RFID authentication protocol, SASI" IEEE Transactions on Dependable and securing computing. Vol. 6,no. 4,pp. 316-320,2004.
[15] Weldhofer, S. Dominikus and J. Wokerstorfer, Strong authentication for RFID systems using the AES algorithm, Workshop on Cryptographic Hardware and Embedded Systems. CHES 2004,volume 3156 of LNCS, pp. 357-370, Boston, Massachuetts, USA,August,IACR,Springer-Verilog,2004.
[16] N.J.Hopper and M.Blum, "Secure human identification protocols",inProceeding of the 7th International Conference on Theory and Applications of cryptolofy-security, pp. 52-56,2001.