VOL. 11, NO. 11, JUNE 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURED COMMUNICATION PROTOCOL FOR NEAR FIELD COMMUNICATION

Saranya and Thomas Niba
Department of Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, India
E-Mail: saranraju30@gmail.com

ABSTRACT

Near Field Communication (NFC) is a rising short-range remote correspondence innovation that offers extraordinary and shifted guarantee in administrations, for example, payment, ticketing, voting and so forth. NFC innovation works for information exchange and empowers the mix of administrations from an extensive variety of utilizations into one single cell phone. The monstrous advantage of the short transmission reach is that it forestalls listening stealthily on NFC-empowered dealings. A few security issues are joined with NFC, which is a major concern. This innovation shows alias ensures protection of clients. It gives contingent security in which personality of clients can be checked by third trusted party (TTP). Issues like MIMT, replay attack, modification attack, session key security convention could settle in proposed with a minimal computational expense increment.

Keywords: MIMT (man in the middle attack), Near Field Communication, session key security protocol.

INTRODUCTION

NFC innovation is powerless against numerous sorts of assaults. Security is hence a standout amongst the most vital issues for the NFC innovation. To improve security, the NFC security guidelines have been proposed to characterize information trade position, tag sorts, and security conventions, e.g., a key assention convention for secure NFC [1]-[3]. For proficient key administration and disavowal among hubs, i.e., initiator and target protests, a Public Key Infrastructure (PKI) is utilized to assemble NFC security principles [4]-[5]. In the PKI base, when two clients need to execute key understanding conventions, they need to trade their endorsements to get people in general key of another gathering. The endorsement is produced by a Certificate Authority (CA) and the client's personality is incorporated into it. Accordingly, the enemy could track the client's activity by following its open key and the client's security might be broken. As a vital security insurance technique, pen name protection assurance strategies have been generally utilized as a part of numerous applications [4]-[9], In such system, the client's character is spoken to by a nom de plume, is produced by the third trusted gathering arbitrarily and has no connection to the client's genuine personality. Along these lines, the foe can't get the client's genuine character regardless of the possibility that he could get the client's nom de plume. Keeping in mind the end goal to ensure the client's protection, Eun *et al.* [10] proposed s restrictive protection safeguarding security convention utilizing aliases NFC applications, Eun *et al.* asserted that their convention could withstand different sorts of assaults. Not withstanding this paper uncovers that Eun *et al* convention can't withstand mimic assaults by investigation as for two unique sorts of assaults. This paper likewise proposes another alias NFC convention to secure the purchaser Internet of things (IOT).

NFC ACTIVE DEVICES

a) NFC peer-to-peer mode

This mode allowing a connection to be made using a different communication protocol such as Bluetooth or WIFI.

b) NFC reader/writer mode

In tag reading and writing mode, where an NFC device can read or change information stored in an RFID tag or contactless card.

c) NFC card emulation mode

As card emulators, providing an alternative storage for information memorized in a plastic card.

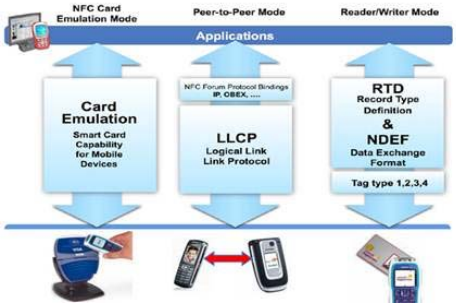

Figure-1. Three communication modes.

OVERVIEW OF ARM7 LPC2148

The LPC2141/2/4/6/8 microcontrollers depend on a 32/16 bit ARM7TDMI-S CPU with continuous imitating and implanted follow support, that consolidates the microcontroller with inserted fast glimmer memory running from 32 kB to 512 kB. A 128-piece wide memory interface and extraordinary reviving operators auxiliary designing enable 32-bit code execution at the best clock rate. For fundamental code size, the 16-bit Thumb mode reduces code by more than 30 % with irrelevant execution

discipline. On account of their minor size and low power use, LPC2141/2/4/6/8 are ideal for applications where downsizing is a key essential, for instance, access control and reason for offer. A mix of serial trades interfaces going from a USB 2.0 Full Speed gadget, distinctive UARTs, SPI, SSP to I2Cs, and on-chip SRAM of 8 kB up to 40 kB, make these contraptions astoundingly suitable for correspondence passages and convention converters, touchy modems, voice assertion and low end imaging, giving both interminable bolster size and high dealing with power. Diverse 32-bit tickers, single or twofold 10-bit ADC(s), 10-bit DAC, PWM channels and 45 speedy GPIO lines with up to nine edge or level sensitive outside impede pins make these microcontrollers particularly suitable for mechanical control and restorative structures.

Figure-2. LPC2148 Microcontroller.

The ARM7TDMI-S processor in like way uses a groundbreaking building framework known as HUB, which makes it in a perfect world suited to high-volume applications with memory confinements, where code thickness is an issue.

SECURITY THREATS RELEVANT TO NFC

Theorem: the proposed security protocol could provide modification key security.

Proof: This includes the erasure, insertion, or modification of data in an unapproved way that is expected to seem veritable to the client. These assaults can be difficult to distinguish. The inspiration of this sort of assault might be to plant data, change grades in a class, modify charge card records, or something comparable. Site disfigurement is a typical type of adjustment assaults.

Theorem: The proposed security protocol could provide session key security.

Proof: Suppose the adversary A could get a session key generated in a previous session. He has to compute if he wants to get the session key in the current session since *A* and *B* generate new random numbers *A r* and *B r* for each session. Then, the adversary has to solve the computational Diffie- Hellman problem. Due to the hardness of the computational Diffie-Hellman problem, the proposed security protocol could provide session key security.

Theorem: The proposed security protocol could withstand replay attacks.

Proof: Suppose the adversary A intercepts the message and replay it to B, where a nonce and a random number generated by A. We also suppose A replay the message 3 MacTag to B upon intercepting the message 2. However, B could find the attack by checking the validity of A MacTag since B generates a new nonce B N for each session. From the similar steps, we could demonstrate that the user A could find the replay attack. Thus, the proposed security protocol could withstand the replay attack.

Theorem: The proposed security protocol could withstand man-in-the-middle attacks.

Proof: we could get that the proposed security protocol could provide mutual authentication between the user *A* and the user *B*. Thus, the proposed security protocol could withstand the man-in-the middle attack.

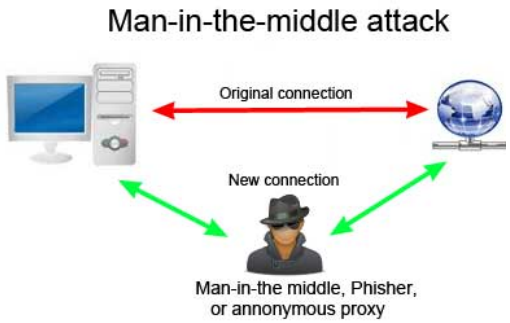

Figure-3. Man in the middle attack.

PROPOSED SYSTEM IMPLEMENTATION

The proposed system consists of ARM 2148 controller and NFC readers. The transmitted hub comprises of smaller scale controller and NFC reader. At first the association between the gadgets can be built up by utilizing the algorithmic steps. The transmitter hub sends the encoded message to the beneficiary hub.

The advanced mobile phone which comprises of NFC module is utilized to encode the message to set up the association. The recipient receives the data and decrypts it and sends it back to the transmitter. If the sender receives the data which matches with its predefined data, the connection will be established. When connection is successfully established, data will be forwarded to the recipient. If the hackers are pretending as actual recipient, they cannot decrypt the data and never sends the data to the transmitter. So Sender can identify the hacker and terminate the connection with hacker.

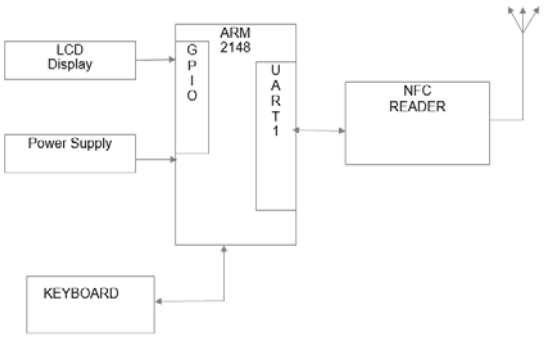

Figure-4. Transmitter node.

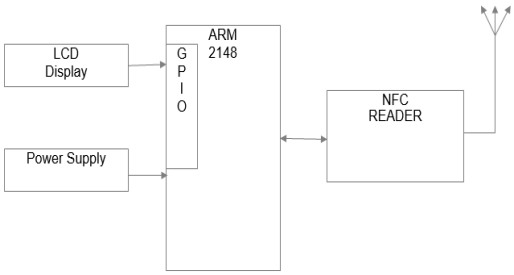

Figure-5. Recipient node.

The following diagrams explain the overall workflow of proposed system.

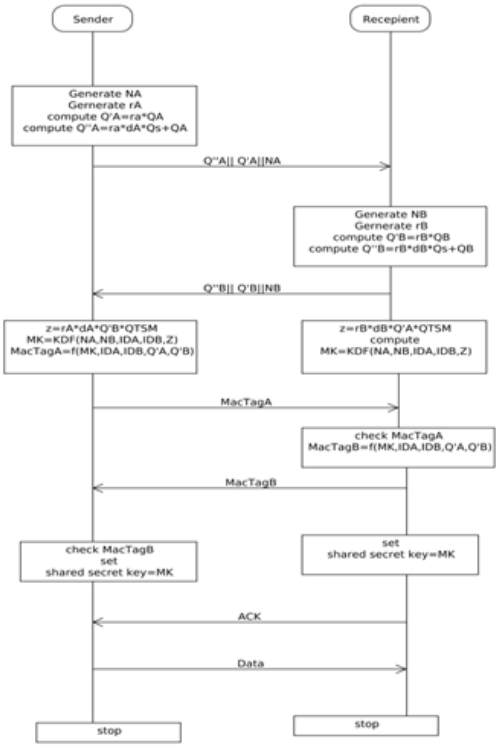

Figure-6. Work process of proposed framework.

EXPERIMENTAL RESULTS

Amid exchange process it will get information from transcient side and check for key to improve the secured information and it will send back to beneficiary information where it will get the information and check for the key. in the event that it is same key then the exchange will be empower orelse it will dishandle consequently.

CONCLUSIONS

In the IoT environment, different sorts of canny gadgets will speak with each other for information gathering and handling and this marvel will prompt the expanded NFC use. In this paper, a nitty gritty examination of the proposed plan regarding different sorts of assaults has been exhibited that demonstrates the proposed convention takes care of the security issues.

REFERENCES

[1] ISO/IEC 15946-1:2008. Information technology - Security methods - Cryptographic methods based on elliptic curves - Part 1: General.

[2] ISO/IEC 13157-1:2010. Information technology Telecommunications and information exchange between systems - NFC Security - Part 1: NFC-SEC NFCIP-1 security service and protocol. ISO/IEC, May 2010.

[3] ISO/IEC 13157-2:2010. Information technology Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[4] G. Calandriello, P. Papadimitratos, J.P. Hubaux and A. Lioy. 2007. Efficient and robust pseudonymous authentication in VANET. Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET 2007). pp. 19-28.

[5] J.C.M. Teo, L.H. Ngoh, and H. Guo. 2009. An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks. Proceedings of the 2009 International Conference on Advanced Information Networking and Applications (AINA 2009). pp. 675-682.

[6] D. He, N. Kumar, J.-H. Lee, R. Sherratt. 2014. Enhanced Three-factor Security Protocol for USB Consumer Storage Devices. IEEE Trans. Consum. Electron. 60(1): 30-37.

[7] J.-H. Lee, J. Chen, and T. Ernst. 2012. Securing mobile network prefix provisioning for NEMO based

vehicular networks. Mathematical and Computer Modelling. 55(1): 170-187.

[8] R. Lu, X. Lin, H. Zhu, P.H. Ho and X. Shen. 2008. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. Proceedings of the 27th Conference on Computer Communications (INFOCOM 2008). pp. 1229-1237.

[9] D. Huang, S. Misra, M. Verma, and G.Xue. 2011. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems. 12(3): 736-746.

[10] H. Eun, H. Lee, H. Oh. 2013. Conditional privacy preserving security protocol for NFC applications, IEEE Trans. Consum. Electron. 59(1): 153-160.

[11] L. Francis, G. Hancke, K. Mayes and K. Markantonakis. 2010. \Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones. In Radio Frequency Identi cation: Security and Privacy Issues, ser. Lecture Notes in Computer Science. S. Ors Yalcin (Ed.). Springer Berlin Heidelberg. 6370: 35{49. ISBN 978-3-642-16821-5. [Online].Available: http://dx.doi.org/10.1007/978-3-642-16822-2 4.

[12] L. Francis and G. Hancke. 2011. Practical relay attack on contactless transactions by using NFC mobile phones. IACR ePrint Archive. Vol. 618.

[13] S. B. Patela and N. K. Jainb. 2013. Near Field Communication (NFC) based Mobile Phone Attendance System for Employees. International Journal of Engineering. 2(3).