Bulletin de la Société Royale des Sciences de Liège, Vol. 85, 2016, *p*. 1475 - 1486

NFC threats and attacks: Applying a low cost algorithm for secure channel using Twofish

Mahmood FATHY[1], Seyed Ali SAMOUTI[2]
[1] Professor Iran university of science and technology, Tehran, Iran , mahfathi@iust.ac.i .
[2] Ali Samouti , Senior IT expert , Iran university of science and technology, Tehran, Iran, Ali.samouti@gmail.com

Abstract

Near Field Communication (NFC) is a new technology which can provide communication between mobile devices in short range. Data would be communicate in three modes: (1) between two mobile systems (MS), (2) MS2 NFC tags (3) reader2MS. One of the must public application in this technology is micropayment system, so by developing NFC technology it would be used in E-commerce and e-everything. In combination of E-Commerce and NFC technology MS would be used as smart card. It is clear that by developing one technology we should consider security and protection system for that. Therefore NFC security and protecting MS from attacks and eavesdropping is so important and critical. In this article at the first we will briefly review about this technology and the architecture, in the next step we will explain about NFC threats therefore we can analyze the attack. After that we will describe some scenarios for protecting against the NFC threats. Then we will explain NFC security standards. In this part we will mention to SSH and SCH , we will show that in secure channel we should use a symmetric algorithm. In this standard AES is has been recommended but we will show that two fish algorithm is more complex than in AES on the other hand we will simulate our proposed approach and we will show that the power consumption and processing time are decreased.

Keywords: NFC, Twofish, power conception, CPU conception

1. Introduction

Today auto identification and collecting their data without human resources is critical, Therefore, we can enter our information in databases in all fields such as industrial, scientific, social and other services. According to this request, Automatic Identification system helps us to response Authentication. Main target for these systems are increasing efficiency and decreasing manual data entry error. However, human can work on other specific major. RFID technology using Radio frequency for identification which is used in recent years for so many applications.[1] Near field communication (NFC) has been derived from RFID. This technology provides connect less communication in short range (around 10 cm). It seems essential that these technologies would be one of the main parts of the MS in near future. There are two structures for NFC implementation: SIM card emulation (NFC would be implemented on SIM-card); NFC has been implemented on the mobile device.[2]

NFC operations can be classified in two parts. Active mode and passive mode as we shown in table 1. This referes to the indicator and target signal. Note that entity which start communication called indicator so If both indicator and target devices , produce signal powers by themselves , communication would be in active mode. But if target devices use power of indicator signal to produce response signal communication, is in passive mode.[3], [4]

Table 1: indicator and target device mode [3]

Indicator Signal	Target Signal	Description
Active	Active	Both devices can produce signals
Active	Passive	RF signal are produced with indicator
Passive	Active	Impossible

Passive devices uses magnetic coupling method for responsing, it means that target device waits for indicator signal. Advantage of this part is that, when the MS device is power off we can use this device applications such as transportation would be efficient and useful.[5]

In active mode RF signal would be produced alternativly by indicator and target devices. Indicator starts communication. Target and indicator produce signals by themselves and send data to the opposite side. As default all the devices are considered as the target mode. Note NFC communication use “listen befor talk” method for avoiding collision. [6]

NFC Data rate are in three type: 106, 212 or 424kbit/s. Also NFC codings have two different types for data transmision. If an active device transfers data at 106 kbit/s, a modified Miller coding with 100% modulation is used. In all other communication Manchester coding is used with a modulation ratio of 10%.[7]

NFC Forum also prepared the specifications for NFC and its services such as NDEF (NFC Data Exchange Format), Record Type Definition, NFC digital protocol, Tag Type, etc. Based on these standards, communication of NFC devices are in three communication modes as we shown in figure 1. Peer to Peer (P2P) mode, Read/Write mode, Card emulation mode. [7]

- Reader/Writer Mode (Proximity Coupling Device, PCD): In this mode, the NFC device can read data stored in another NFC compatible passive tag without using battery. Such tags can be found on Smart Posters or curriculum scheduling in university or on E-MAP in the entry of a city allowing the user to store required information by reading the tag with the NFC device in their cell phones.
- Card Emulation (Proximity Inductive Coupling Card, PICC): An NFC device can also act as a smart card after has been switched into card emulation mode (ISO14443 like an RFID). In this case an external reader can read the NFC device as the same as a smart card. This mode is useful for electronic-payment and electronic truism. [8]
- Peer-to-Peer (Near Field Communication, NFC): The NFC peer-to-peer mode (ISO18092) allows two NFC active devices to achieve a bidirectional communication to exchange contacts, Bluetooth pairing information or other information. To establish a connection a client (initiator) is searching for a host (target) to setup a connection. [9]

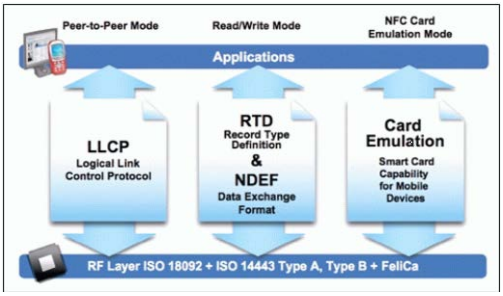

Figure 1: NFC Communication Modes [7]

In another classification, NFC operations are classified into three sections: [8]

1. Communication between MS systems in HDX mode NDEF (NFC Data Exchange Format)
2. The Communication between Ms and reader : it is similar to the peer to peer mode.

3. Communication between Ms and tag : In this case by integration of NFC and other network devices such as 4G cellular system we can save the ticket in MS, so MS is emulated as tags and is connected to the another reader.(figure 2)

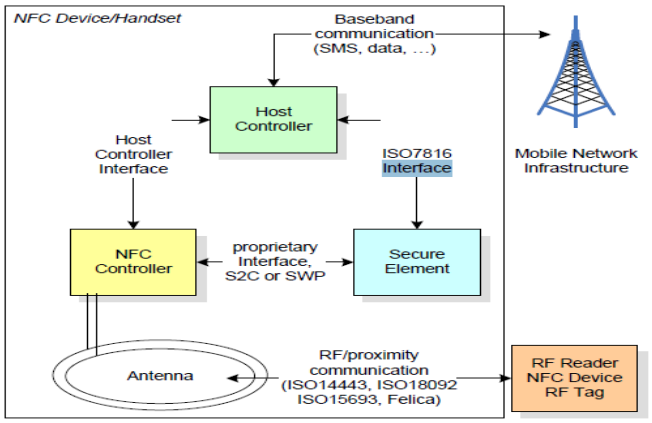

Figure 2: Architecture of NFC integrated in a mobile device [9]

Figure 3 shows that how a call setup step will be step is done in an NFC in NFC communication for NDEF or PCD mode. As you see the indicator sends the first signal to the target :[10]

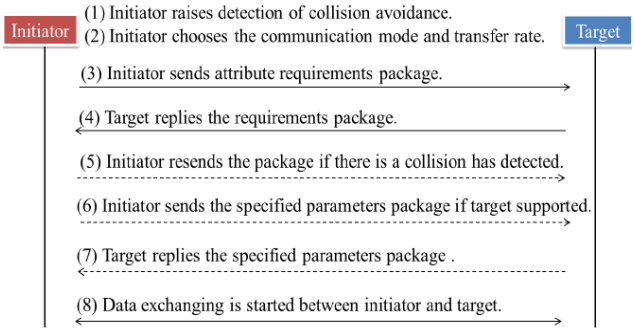

Figure 3: Call set up for NFC communication[9]

2. SWOT analysis for NFC application

Strengths, Weaknesses, Opportunities, and Threats [SWOT] analysis for NFC examine strengths and weaknesses of a product internally and emphasize the opportunities and threats of the external environment. Regarding to this technology we should clarify threats and opportunities.In table 2 we show summary of SWOT for NFC .[11]

Strengths: What is the strength of using this technology? Main strength of this technology is High distribution rate because of penetration level of mobiles and somehow Economies of scale. Secondly, we can talk about High compatibility (NFC compatible to use on mobiles), Range of NFC applications and at last ease of use of NFC is strength of NFC SWOT, because NFC is found everywhere and is Faster and more convenient then other technology.

Weakness: What weakness do we need to remove from NFC technology? First of all, we should consider that how NFC could have be adverse effect on phone like reducing the life of the battery and second we should mention the security and privacy risk for example virus attack or hacking and information misuse are amongest main problems. Also Costs is another weakness because phones with NFC cost more and in other hand infrastructure deployment and service cost so much.

Opportunities: What opportunities would be preparing? Technology innovation is critical opportunity because of customer loyalty and first mover advantages to new innovation.

Then we can point on other business opportunities for example strategic partnerships or increase in customer interaction in a new application are another opportunity.
Threats: What threats do we need to consider? attack related to new technology as we will discuss, is main threat for example Lack of business models or Lack of laws and regulations or reluctance of change are amongest main threat of new innovation, secondly competition with other technologies is another threat. In this article we will focus on threat and prepare solution for weakness.

Table2: Advantage and disadvantage of NFC mode communication[12]

	P2P mode	Card emulation mode	Reader /Writer mode
Standard	ISO/IEC 18092	ISO/IEC 14443	ISO/IEC 14443
Advantage	Connection speed less than 0.1s .	Combine many digital valued card in one phone	It can read tags information in darkness and contact soon
Disadvantage	Transaction speed is 424kbps which less than Bluetooth 2.1MB/s	The content of card can be read by others when mobile phone is out of battery or in the turn off status .	The price of the active tags is high. It need more cost for mass production than produce QR code tag
Application	Exchange business card , shared information , game application	E-passport , mobile payment , check in and member identification	Museum guiding, transportation tokens , turn on / off some function on the phone quickly

3. NFC standard

Figure 4 shows all the standard taht we describe in bellow context,

(1) ISO/IEC 18092 Standard[12]

This standard submitted as the draft to the ECMA (European Computer Manufacturers Association). After ECMA had examined the draft passed, it had been accepted into the International Standard Organization. This ISO/IEC 18092 standard is the current standard for NFC technology.

(2) ISO/IEC 14443 Standard [12]

It defines the connection standard and transmission protocol between reader and PICC on mobile phones. It mainly operates the wireless HF activities on 13.56MHz, like RFID or MIFARE tag. There are three transmission modes in NFC which named NFC-A, NFC-B and NFC-F which is the FiliCa contactless IC card transmission technology.

(3) ECMA 385 and ECMA 386 Standards[13][14]

They support two services which are Secure Channel service (SCH) and Shared Secret service (SSE). The structure of ECMA 385 has been accepted as the Open System Interconnection Reference Model.

Also in other document and forum we can find bellow standards too: [3]

ECMA-340 “NFC Interface and Protocol (NFCIP-1)”,ECMA-352 “NFC Interface and Protocol(NFCIP-2)”, ECMA-356 “NFCIP-1 - RF Interface Test Methods”, ECMA-362 “NFCIP-1 - Protocol Test Methods”, ECMA-373 “Near Field Communication Wired Interface (NFC-WI)”

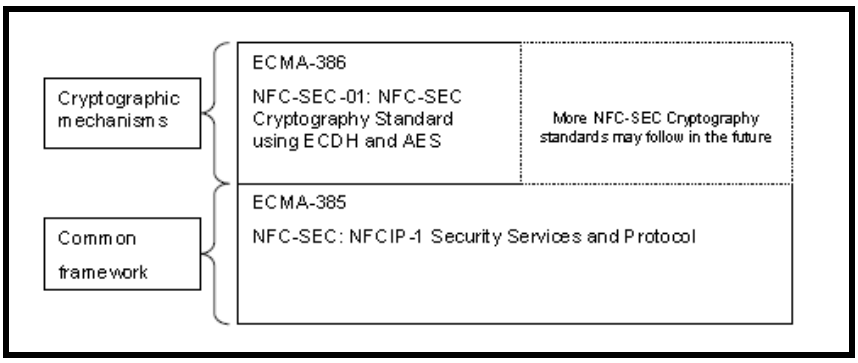

Figure 4: NFC security standard [3]

NFC-SEC as illustrated in Figure 5 uses the OSI reference model specified in ISO/IEC 7498-1.[14]

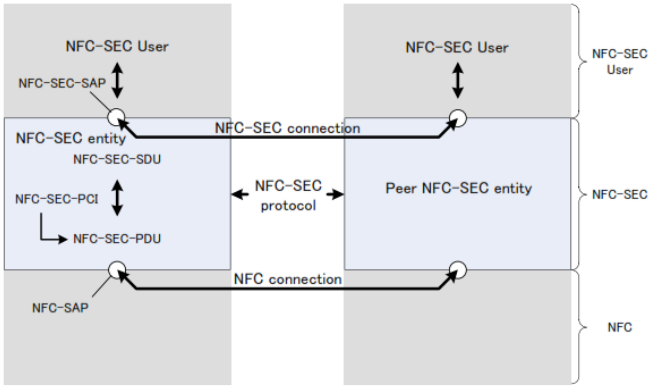

Figure 5: NFC security (ECMA 385)[14]

NFC-SEC entities obtain NFC-SEC-SDUs (requests) from NFC-SEC Users and return NFC-SECSDUs (confirmations) to them. This Standard specifies the Secure Channel Service (SCH) and the Shared Secret Service (SSE). To provide NFC-SEC services, Peer NFC-SEC entities exchange NFC-SEC-PDUs by conforming to the NFC-SEC protocol over NFC-SEC connections.

Peer NFC-SEC entities send and receive NFC-SEC-PDUs through NFC Service Access Points (NFC-SAP). A NFC-SEC-PDU consist of NFC-SEC Protocol Control Information (NFC-SEC-PCI) and a single NFC-SECSDU. This clause specifies two services, SSE and SCH, that NFC-SEC provides to the NFC-SEC User. When invoked, these services enable the cryptographic protected transmission of NFC-SEC User messages between the peer entities by means of a protocol. Shared secrets established with the services specified below shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards.[18]

Shared Secret Service (SSE): The SSE establishes a shared secret between two peer NFC-SEC Users, which they can use at their discretion. Invocation of the SSE shall establish a shared secret by the key agreement and key confirmation mechanism according to the NFC-SEC cryptography part that defines the PID. [19-21]

Secure Channel Service (SCH): The SCH provides a secure channel. Invocation of the SCH shall establish a link key, by derivation from a shared secret established by the key agreement and key confirmation mechanisms, and shall subsequently protect all communications in either direction across the channel, according to the NFC-SEC cryptography part that defines the PID.

4. NFC Threat analysis

We can divide NFC threats in 2 parts as we shown in table 3: 1)Physical and Denial of service threat 2)Privacy attack.

Privacy attack is done be have done in several ways such as :

Eavesdropping: Communicate between two devices over NFC channel can be eavesdropped or received by an un-authorized device. The attacker can use larger and powerful antennas to receive the communication information. This enables the attacker to eavesdrop an NFC Communication over greater distances. [15]

It is important to highlight that passive mode data transmission is somehow difficult to be attacked on compared to active mode. Only solution to this type of threat is to use a secure channel (SCH). The communication over NFC channel should be authentication based.[3,15,16]

Eavesdropping in the Peer-to-Peer mode (NDEF): in the Peer-to-Peer mode, it has some risks for sniffing by attacker. Because it is communication channel without security protection, so hacker can get the data from radio signal. Eavesdropper can use the jammer to disorder the communication or get information or data when two devices are in the NDEF. However, users would use (SSE) and (SCH) in the P2P mode. [3,12]

Eavesdropping in the Card Emulated (PICC): if an enable NFC system in mobile phone is not in use, the content of NFC card still can be reached by attacker. Identity Authentication is the same as P2P mode : (SSE) &(SCH) can be used to protect the data transmission.[3,5,12]

Data Corruption The data corruption can be considered as DoS[1] if the attacker replace data to an unknown format because of this, the communication between the sender and receiver will be disturbed. Even if it is only an error message, this is simply a way to kill the device also there should be kind of processes by the user to turn on.[9] NFC devices are designed to be able to detect RF fields in which they communicate (listen before talk). Another way to corrupt the data can be by transmission of the same or valid frequencies at the time when communication is handle on .This sort of corruption can be run by software which installed on the same smart phone in background.[16,17]

A powerful device is needed than the typical power of the RF device to corrupt indicators data. The powerful signal could be easily detected by the NFC devices. These types of attacks are easily detectable.[15] Solution: we can encrypt data or is recommanded to use CSMA/CD, prepare log server report for operator when there is no response from target tag.

Relay data transferred over the RF: both ISO14443 and ISO18092 are open for relay attacks. Which cannot detect by the card or reader. Note that another point is called battery-off mode. In this case the smart card capability even has been relayed if the battery was removed from the device. From the current approach a button on the device to turn on tag emulation would be a sufficient solution. It is an easy and suitable way for devices which provides a sound security, regarding replaying, skimming and also tracking and tracing.[3] Solution: we can use encryption and random ID for hand shaking in SSH/SSE.

Data Modification: Invader changes the actual data with valid but incorrect data. So we would have Non-integrity communication. (corruption + modification) The receiver in this case receives data change by the attacker during transmission. In this case attacker can play and handle the amplitude modulations of the transmission which should be start up.[12, 16] Solution: use an Integrity message algorithm (SSE)

Data Insertion: Unwanted data can be inserted and forward to the target device in the form of messages on communication link by an attacker. The success of attacker depends upon the duration of communication if communication time is so long attacker would be having better chance. A possible countermeasure is possible if the answering device responds to the first device without a

[1] Denial of service

delay. The attacker does not get the window to insert malicious or manipulated data.[17], [3] Solution: Digital signature would be use full for this part. (SSH)

Man-in-Middle Attack: in Man-in-the-Middle Attack, third party tricks the two main connection parts in other hand this device routs the communication between the indicator and the target to go through the third party. We find that in NFC technology Man in the middle will not occurred.[17]

Relay Attack: in this attack the attacker uses another communication link (relay) as a mediator to increase the range. The attacker needs no physical access to the device, but only an antenna and the relay device in reading range.[3] Solution: monitor the signal and signal range analysis.

High Distance Read The attacker modifies an NFC capabilities device so he/ she increases antenna range, therefore, he/she can read tags from a safe distance. This is not easy, but there is another way too. The attacker must increase the energy of the signal field, use an optimized antenna and handle the increasing noise in the communication. [15] Solution: monitor the signal and signal range analysis lock the change functionality in MS.

Social Engineering: ON NFC communication channel where other devices can connect to the NFC (contactless), is easy to use either a malignant card or a sundry reader to carry out unwanted operations.[15] . Solution: Digital signature would be helpful for this part. (SSH) , Only allow our NFC device communicate with authorized signed cards and readers.

Destroy: This is the simplest attack which could be used. By using this attack, the tag is not able to continue communication. It is like DoS or corruption attack. It could be happened by mechanically, for example by cutting the antenna connection or overpowered electrical field on the tag's working frequency, so that the electrical components would overload. This attack would compromise the availability of an NFC system.[15]

Shield: This attack is provisory and it can happen when we placing the tag inside a metal box or a wrapping it in tinfoil. The tag is not destroyed permanently. This attack would compromise the availability of an NFC system.[2]

Clone: in this attack the original tag is read and an exact copy is created. Some papers show that this attack is same as relay attack, the complexity of attack depends on the tag security and accessibility. A read-only tag (ROT) which stores only a simple ID can be cloned very easily. There are also simple solutions to change the ID. The reader cannot detect if it is the original or the cloned tag. If some kinds of certification is used, this attack would get more complex and unsuccessful. This attack compromises the secrecy of an NFC system[15]

Falsify/Replace: This attack overwrites the data or physically replaces tags data. ROT2 data tags cannot be replacing but ROW3 data tags can be threat by this attack. Overwriting can be done easily if the original tag is a writeable note that tag without any security mechanism would be weak for this attack. The aim of this attack is for phishing purposes. This attack compromises the integrity of an NFC system.[5]

Tracking: Tag always uses the same unique ID for anti-collision (or is a simple read only tag with a numeric ID). An attacker could track the tag easily. If the tag is always carried by the user, his movements could be tracked. This attack compromises the secrecy of an NFC system.[3]

Phishing: protection of touching a tag or a reader with the mobile phone is probably much lower than wired connection. So phishing attacks could easily be applying by replacing or modifying tags. This is a simple and inexpensive way to reach NFC tags data. Using signatures on tags and transporters would be suitable way to overcome this issue.[15]

[2] Read only tag
[3] Read or Write

Spoofing: The tag data can be duplicated and transmitted to a reader. All RO and RW -transponder which do not use encryption algorithm are in danger; in addition, it cannot be detected by the reader device.[7] Solution: we can use random code or encrypt ID.

Table 3: corresponding operating mode and NFC threat[12]

Operating Modes	Attack
Card Emulation mode	Denegation of attack
	Eavesdroping in the card emulated mode
	Relay Attack
Reader Writer mode	Identity Authentication
	Phishing attack
	Ticket cloning

5. Overview on twofish algorithm

Twofish is a 128-bit symmetric block cipher and can accept a variable-length key up to 256 bits. The cipher is based on a Feistel algorithm, has 16 rounds, a F function made up of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix over GF, a pseudo-Hadamard transform, bitwise rotations, and a well-designed key schedule. The algorithm can be optimized for use with regard to the hardware platform:

- An optimized implementation of Twofish can encrypt on a Pentium Pro at 16.1 clock cycles per byte
- An 8-bit smart card implementation encrypts at 1660 clock cycles per byte.:[21]

Twofish was designed to meet NIST's general design criteria for AES [NIST97b], which are:

- Key lengths: 128 bits, 192 bits, and 256 bits.
- Efficiency, both on the Intel Pentium Pro and other software and hardware platforms.
- o No weak keys and Flexible design: accept additional key lengths, suitable for a stream cipher, hash function, and MAC , implementable on a wide variety of platforms and applications
- Simple design: ease of analysis and ease of implementation. To increase the capabilities and the security of the Twofish algorithm the designers have also imposed the following performance criteria on their design:
- Accept any key length up to 256 bits, Encrypt data in less than 500 clock cycles per block on an Intel Pentium, Pentium Pro, and Pentium II, for a fully optimized version of the algorithm.

Because of the benefits which we considered, we simulate Twofish algorithm for NFC and in our simulation we find that we can have decreases power consumption and process consumption. we simulate this encryption in machine which similar to the mobile.

A hybrid system in term of NFC system requirements that is best suited for lightweight cryptographic method. In the future, we would like to design the system with even more complex properties to make it even harder to decrypt without authorization and has lower power and CPU consumption. We would also like to increase the scope of the project by including more type of files as input with unlimited size. [22]

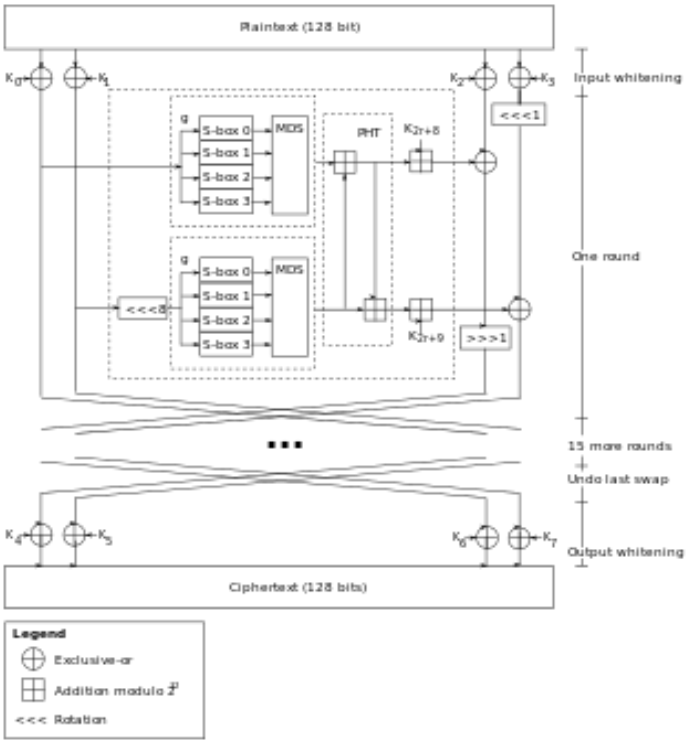

Figure 6: Twofish algorithm [20]

6. Using twofish for NFC [3]

We simulate with C# for calculating of time encryption and throuput and process consuption and power consumption .
Our simulation is simillar to the regular cell phone (CPU and RAM). Also we use encyption algorithm which is used in other simulations . we found bellow result :

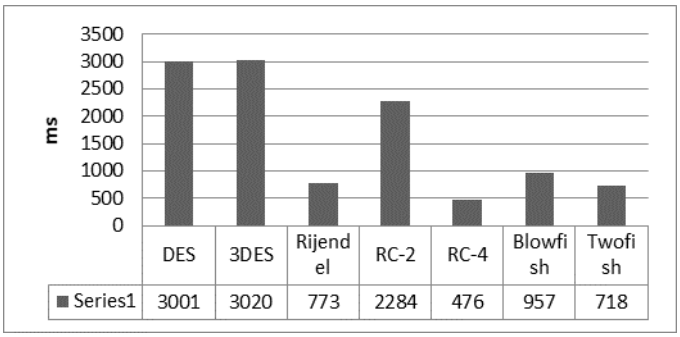

Figure 7: Encryption time for symmetric algorithm [3]

As you see in figure 7, encryption time for small text file is shorter than AES also when we use this algorithm for 100 times and we consider power consumption when we use Twofish algorithm, we find that power consumption decreases about 15% .

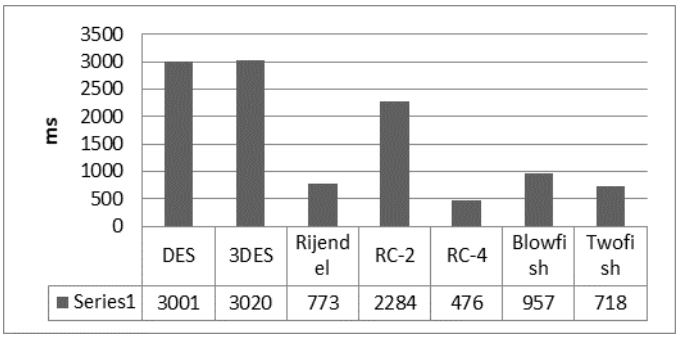

Figure 8: Data rate in symmetric encryption algorithm [3]

As you see in figure 8, data rate of twofish is smaller than AES, as we mentioned in NFC we want to communicate small files and this difference would be appearing for small files but in large files it should be change as you see in figure 9.

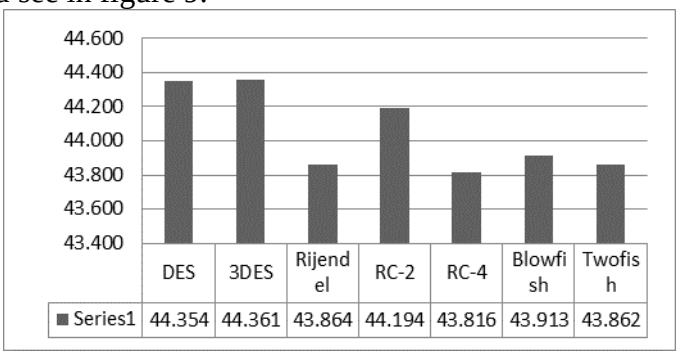

Figure 9: Data rate in symmetric encryption algorithm for larg files [3]

In figures 10 11, 12 we shows the comparison of key length, as we show for each application we can use difference key lengths.

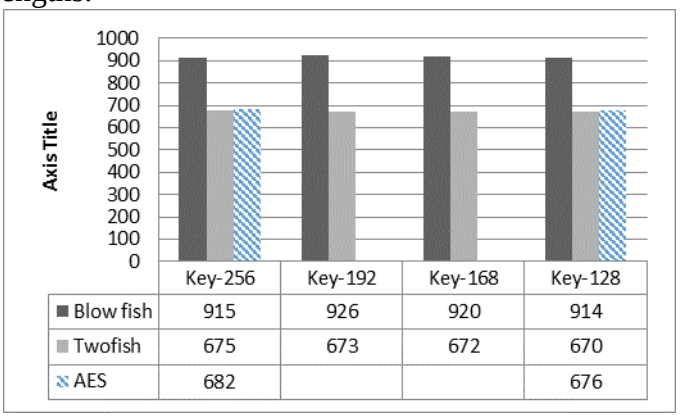

Figure 10: comparing key lengths and encryption algorithm

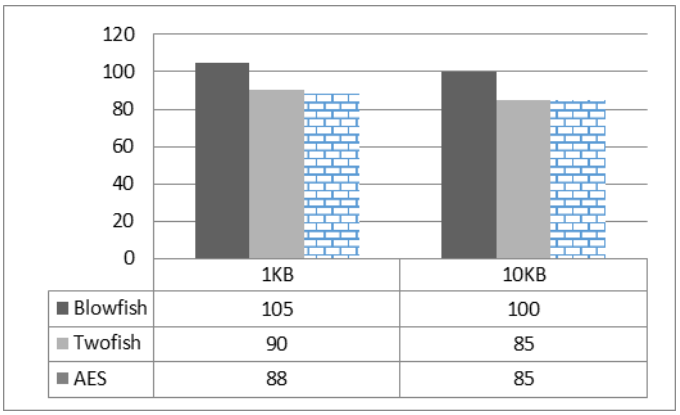

Figure 11: power consumption for text file

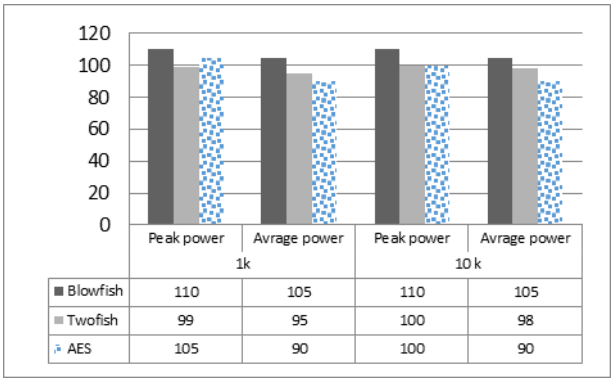

Figure 12: Average of power consumption of 2 files

7. Conclusion

In NFC technology, there are many security issues should be considered as discribed in this paper. One of the must important note in mobile technology is battery gap. So we should consider low cost algorithm. Twofish algorithm would be helpful for NFC technology and it could be replaces as AES . We suggest to work on SSH and SCH for feutures work.

REFERENCES

[1] S. Ahson, "RFID hand bookapplication" , technology , security and privacy, Teylor group, 2008.

[2] S. Ahson, "Near field communication hand book", CRC press, 2011.

[3] M. Fathy, A.Samouti, "Analysis , compare and develop the Encryption methods for eavesdropping in Near Field Communication (NFC)", Msc thesis , University of IUST, 2013.

[4] V.A.K, "Near Field communcation," S.D.M college Dharwd , Belgaum, 2013.

[5] A. Antoni Jara, "Evaluation of the security capabilities on NFC powered devices", University of Murcia , 2012.

[6] K.B.Ernest, "Security in near field communication," Asutria , 2011.

[7] J. Baek, "Secure and Lightweight Authentication," in 10th Asia confernce on Information security , Malysia , 2015.

[8] J.SBo.Yaang, "Near Field Communjcation technology," Linkopings University, MSc thesis, 2013.

[9] G. Maldmayer, "NFC devices : Security and privacy," in The third international conferance on Avalability , Relability and security , 2009.

[10] J. Madlmayr, "Risk Analysis of OTA transaction in an NFC Ecosystem," First international conferance on NFC, 2011.

[11] F. Mehmood, "Analytical investigation of mobile NFC adaption with SWOT-AHP," in The 7th International Conference Interdisciplinarity in Engineering, Eng, 2014.

[12] C.-H. Chen, "NFC Attacks Analysis and Survey," in 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2015.

[13] N. Frum, "NFC-SEC ECMA-386," NFC frum, 2012, 2012.

[14] N. Frum, "NFC-SEC ECMA-385," NFC Frum, USA, 2011.

[15] N. B.Thorat, "SURVEY ON SECURITY THREATS AND SOLUTIONS FOR NEAR FIELD COMMUNICATION," in IJRET: International Journal of Research in Engineering and Technology , 2014.

[16] H.S.korrtvedt, Securing Near Field Communication, Norwegian: Master of science , 2010.

[17] A. E. Dia salma, Eavesdroping Near Field Communication, Noorweigan Information security conferance , 2012.

[18] N. Frum, "Logical Link Control Protocol," NFC Frum, USA, 2013.

[19] M.Kilas, "Digital signitures on NFC tags," Master of sicence SebastienPierrel Ericsson, 2010.

[20] H. paul, “twofish encryption algorithm”, Security Asia conference , 2005.

[21] F. Behrouz, Cryptography and network security, MC-Growhill, 2008.

[22] D. Bhardwaj, "Efficient Hardware Encryption Using Lightweight Process," in International Journal of Science and Research (IJSR) , 975-94 .

[23] A. Tamimi, "Performance Analysis of Data Encryption Algorithms", 3rd IT conferance , Malysia , 2009.

[24] w. stalling, Cryptography and Network Security, Prentice Hall, 2015.

[25] S.Stones, "Mobile Near Field Communication (Mobile NFC)," Silance 18, 2009.

[26] M.Kerschberger, NFC a survey of safety and security measures, Msc thesis , University of Vienna , 2011.