Optimized Conditional Privacy Preservation Protocol for NFC Applications using Genetic Algorithm

Baldeep Singh
ECE
UIET Panjab University
Chandigarh, UT India

Arvind Rajput
Assistant Professor ECE
UIET Panjab University
Chandigarh, UT India

Sabhyata
Assistant Professor ECE
UIET Panjab University
Chandigarh, UT India

ABSTRACT

In the recent years the NFC with the combination of smart devices has widened the utilization range of NFC. It is said it will replace the credit card in electronic payment so security is one of the area that is to be checked. Currently the NFC security requires user's public key with the fixed value which contain the message. The attacker can create a new profile of the user by using their public key and thus the privacy of the user is compromised. In this work, network environment can be generated using 50 nodes. User can select source and destination node and then simulation can be done on the basis of proposed algorithm. The conditional privacy protection based on multiple pseudonyms is used to solve the issues generated in NFC environment. This work is to optimize the above environment by using optimization algorithm. Genetic algorithm which is artificial intelligence based algorithm is used in this to reduce the storage requirement, average delay, packet drop ratio and improve the network's throughput.

General Terms

Security, Near Field Communication, Genetic algorithm for optimization.

Keywords

NFC, Security, TSM, Pseudonyms, Throughput, Storage Requirement, Packet Drop Ratio (PDR), Average Delay.

1. INTRODUCTION

Near field communication (NFC) is a set of standards for smart phones and similar devices to generate radio communication with one another by different means like by touching them with one another or by bringing them into proximity i.e. no more than few centimeters. Anticipated applications and Present have contactless data exchange, simplified setup and transactions, of more complex communications such as Wi-Fi. Communication is also possible between a NFC device and an unpowered NFC chip, called a "tag". In ISO 18092 details of NFC specification can be found [1]. NFC main character is that it's a wireless communication interface with a working distance limited to about 10 cm. it could be operated in different modes. The modes are differentiated either it create its own RF field or by retrieving the power from RF field generated by another device [2]. Active devices are the devices with generates their own field if not then is it known as passive device. Active devices mainly have their own power supply where as passive don't. Three different configurations are possible when two devices communicate with each other.

Currently, NFC technology is treated more as an input mechanism for launching other communications technologies than as a radio type for actual data transfer in targeted use cases. While the NFC technology supports extension mechanisms for transfer of large amounts of data, the current radio frequency allocation to NFC requires close proximity of NFC devices during interactions, which creates a user experience that is not conducive to long data transfers. This is why NFC is typically expected to be used for either small data transfer interactions or for launching larger data transfers with an alternative mobile wireless communication technology, such as Bluetooth, WI-Fi, and mobile data service [3].

NFC provides a capability for initiating wireless communication interactions. There are four main reference use cases for these interactions:

- Service initiation (e.g., read a "smart" tag on a poster to acquire information, or to launch a web browser and exchange for product discount coupons)
- Pairing of devices (e.g., send a camera photo to a printer, or activate a Bluetooth headset by tapping on the mobile accessory)
- Peer-to-peer data transfer (e.g., quickly transfer information between mobile devices with a simple touch, such as to exchange business cards or play a multi-player game)
- Secure NFC card (e.g., mobile device acts as an access, loyalty, or payment contactless smart card that is read by others)

The UID (unique identifier) element in NFC tags is subject to the potential threat of tampering and spoofing. The typical mitigation of this threat is to provide a tamper-resistant "seal" and to sign the object with a credential from a trusted authority, thus providing a reference of authenticity for recipient entities. The NFC Forum specifications include a framework for signing multiple NFC data exchange format records (NDEF) in NFC tags, to help assure that the originator of the tag and its information are trusted. However, NFC ecosystem participants might additionally consider agreeing on a set of reference certificate authorities (e.g., providers of root certificates) and also adding the signature framework to their NFC interoperability certification for use in future products and services [4].

Additionally, NFC standards should be periodically reviewed with the intent of new work items to supplement the stack of specifications with additional standards or implementation profiles to address identified gaps in the current version of these standards. For example, as noted above, current NFC standards do not completely provide a common approach to ensuring the authenticity of NFC tag data. For example, a digital signing approach could be standardized to help ensure that the originator of the tag and its information is trusted and not tampered with.

2. RELATED WORK

Hasoo Eun et al. [5] have explained that various mobile terminals equipped with Near Field Communication have been released in recent years. With smart devices combining with NFC it has widened the utilization range of NFC. Credit cards in electronic payments might be replayed by NFC. So for vitalize the electronic payment the security issues are required to be checked. Presently the NFC security standards which are used require the user’s public key in the process of key agreement at a fixed value. Fixed element contains the occurrence of message like a public key of NFC. By collecting the related message from the users public key an attacker can generate a profile. Privacy of the user’s can be compromised and they could be exposed via the created profile. To solve this problem this paper proposes a conditional privacy protection methods based on pseudonyms. For conditional privacy Protocol Data Unit is defined. Users can tell the other party about their communication according to the protocol defined i.e. by sending the conditional privacy preserved protocol data unit through NFC terminals. This method succeeds in minimizing the computation overhead and update cost by taking advantage of the physical characteristics of NFC.

Roy Want et al. [6] have described that it is a critical time for manufacturers that are thinking about including NFC in mobile devices. The NFC standards and technical specifications are in place, and open source NFC stacks are available for Linux, Android, Windows, Win/Mobile, and embedded real-time operating system solutions (www.open-nfc.org). Samsung has made the first move with its Android NFC Smartphone. It’s perhaps only a matter of time before NFC becomes another “must have” feature for mobile devices.

Jeffrey Fischer et al. [7] for the vast users of cell phone a creation of a new paradigm is been promised by Near-field communication and it is emerging to be a near-term reality. The merging of cellular telephony and RFID will bring along a wealth of new application along with it. The security mechanisms, human interface and application space are maturing; the payment companies and the service provided are working to keep up with the new capabilities; and it is started to be implemented in the cell phone design of new generations. Electronic companion have become magic wands with the use of NFC. The basic “wand” indicates intent. Where u point, whom u point or when u point, tell the machine part of human-machine interface about what it is supposed to do. Because the near-field RF operation places severe limits on the range, the RF connection that results from the proximity of the phone and another NFC product indicates that the user really meant to do something; it indicates their intent. Early skepticism about unleashing too much “intent-based operation” in the phone seems to have been stayed by real-life demonstrations brought to us by the visionaries of this technology. The landscape of new electronic capabilities can only be characterized as vast and driven by impressive creativity. The technology has also passed the early adoption test. Deployments of proximity cards for transportation and payment in Western Europe and Asia have been so overwhelmingly successful that it has brought about significant investments geared toward coalescing standards and specifications, and migrating the technology into cell phones. NFC operates on the same RF principle as proximity cards. There are several advantages of integrating the solution into the cell phone. One obvious advantage is the “Swiss Army knife” approach to centralizing a user’s daily life. Another is that the phone affords a more capable engine than a card for enabling higher-level functions that demand greater memory and processing. Third, and most powerful, is that it provides a backend connection to the cellular network for high-level operations such as real-time loading of funds, security management, and telephone and Internet connections driven by inputs received from NFC interactions.

Florian Michahelles et al. [8] have described that RFID is attracting enormous interest as it quickly becomes a widely deployed pervasive technology. At the PERTEC (Pervasive RFID/Near Field Communication Technology and Applications) workshop on 19 March 2007 (part of PerCom 2007), about 30 researchers from Europe, Asia, and the US discussed issues in this field. Topics included management of data ownership in supply chains generated through RFID, integration of RFID and sensors, security and privacy, NFC applications, RFID-based location sensing, and emerging research challenges.

3. DESIGN & IMPLEMENTATION

This work focuses to implement the Genetic Algorithm in Privacy Preserving Protocol to optimize and reduce the storage requirement. Previous studies developed an optimized method for secure communication with NFC structure with multiple pseudonym based method and provide conditional PDU for further privacy of personal communication of user. For providing pseudonym which are essential for maintaining secure identification of the user which could be very useful in avoiding man in middle attack. Multiple pseudonym assigned by Trusted Service Manager is a big advantage but lacks in storing, processing and communication cost. Normally for storing, independent structure are applied to provide uninterrupted security. In this work, optimizing of this is done by solving the issue of storage by using Genetic Algorithm which is artificial intelligence based algorithm [9].

3.1 Proposed Model

The proposed model focuses on following objectives which are helpful in improving the efficiency of the system by reducing storage requirement and are practically implemented using NS-2 Simulation environment.

a) To Generate Network scenario by using NS-2 simulation environment.
b) To propose a new algorithm/method for storage reduction based on GA.
c) To modify the GA algorithm by using new fitness function based on mean and grand mean.
d) Compare this technique with the current state of art techniques.

In this proposed work, a network scenario of 50 nodes is generated. User has a option to select source & destination node. Communication can be take place only between the selected nodes. The result obtained has decreased the storage size, delay and packet drop ratio & has increased the throughput.

3.2 Basic Block Design

Condition privacy preserving protocol have developed an optimized method for secure communication with NFC structure with multiple pseudonym based method and provide conditional PDU for further privacy of personal communication of user for providing pseudonyms, which are essential for maintaining secure identification of the user, could be very useful in avoiding man in middle attack.[10] Multiple pseudonym assigned by Trusted Service Manager is big advantage but lacks in storing, processing and communication cost. Normally for storing, independent structure are applied to provide uninterrupted security. In this work, optimizing of this is done by solving the issue of storage by using Genetic Algorithm which is artificial intelligence based algorithm. Genetic algorithm is used which helps to reduce the number of pseudonyms to store. It means it helps in selecting the appropriate or required pseudonyms for storing. Fig 1 shows the basic design of the system.

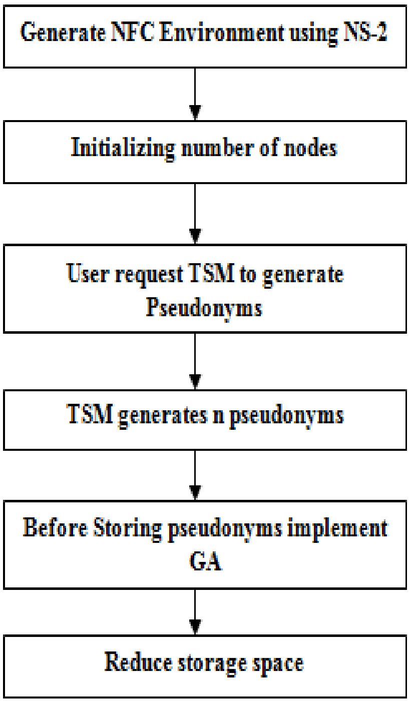
Generate NFC Environment using NS-2
Initializing number of nodes
User request TSM to generate Pseudonyms
TSM generates n pseudonyms
Before Storing pseudonyms implement GA
Reduce storage space

Fig 1: Basic Design of the System

3.3 Algorithm Level Design

Step 1: Generate Network Environment

In this work, simulation environment can be generated by initializing 50 nodes in the scenario. From these all 50 nodes one node is act as a base station and other one act as certifying authority. All left nodes were used for communication. Fig 2 shows the generated scenario in NS-2 [11].

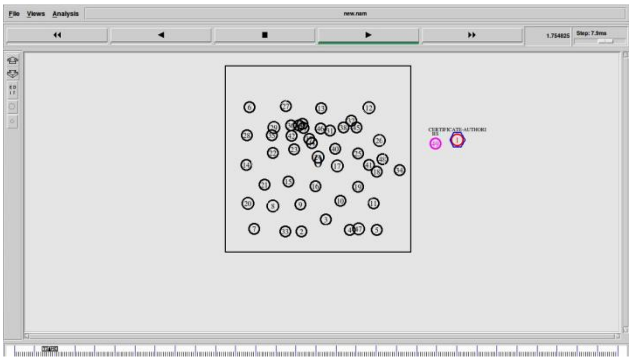

Fig 2: Network Scenario of 50 nodes using NS-2

Step 2: Request for Pseudonym Generation

Firstly user requests TSM for pseudonyms. TSM generates n pseudonyms and transmit it to user. Then, the TSM stores the transmitted pseudonyms and ID of user. A pseudonym composed of public key, private key (that is encrypted with long-term public key of user), ID of the TSM, and signature of the TSM. In this work before storing transmitting pseudonyms a genetic algorithm is implemented [12].

Step 3: Implementation of GA

- GA first counts the number of transmitted pseudonyms and generate random population of it.
  Rand_pop = [1 X (no. of pseudonyms)]

- Calculate fitness value using Mean & Grand mean values of this rand_pop.

$$M_0 = \frac{1}{N}\sum_{i=1}^{L} N_i M_i.$$

  Here M_0 is mean value of the random population.

$$M_i = \frac{1}{N}\sum_{j=1}^{L} W_j^i\ , \qquad i = 1,2,3\ldots., L$$

  Here M_i is grand mean value of the random population.

$$fitness\ value = \sqrt{\sum (M_i - M_0)(M_i - M_0)}$$

- Convert number of pseudonyms into binary number. For example, let number of pseudonyms are 835 then binary number for this is:
  1101000011

- Crossover
  Probability of crossover pc=0.6;
  Best_fit = fitness value

Now crossover point (cpoint) is defined as pc* best_fit.

$$cpoint = roundof(pc * bestfit)$$

From the above equation, cpoint results as either 1 or 0.
For binary number 1101000011

If cpoint = 1

Then after crossover values returns as 1101001001

Else if cpoint = 0

Then after crossover values returns as 0111000011

- Mutation

  Probability of mutation pm=0.6;
  Best_fit = fitness value

Now mutation point (mpoint) is defined as pm* best_fit.

$$mpoint = roundof(pm * bestfit)$$

From the above equation, mpoint results as either 1 or 0.

If mpoint = 1

Then after mutation values returns as 0101001001

This binary value is equivalent to 451.

Else if mpoint = 0

Then after mutation values returns as 0111000011

This binary value is equivalent to 329.

- Now TSM have to store only those pseudonyms which can be selected after mutation.

From the above example it is clear that after applying Genetic Algorithm number of pseudonyms get less as compare to the original pseudonyms which need less storage space.

4. RESULTS

The results are based on the simulation of the scenario defined and performance analysis is based on some performance matrices like packet drop ratio (PDR), Throughput, Storage size and delay. The results show the all the above define matrices calculated from the trace file generated by ns-2 simulator for previous and proposed work. Fig 3 shows the resultant throughput generated by both previous and proposed method and proves that proposed work has higher throughput as compare to previous.

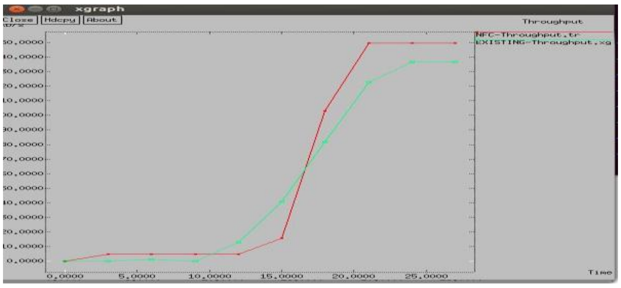

Fig 3: Throughput

Table 1: Throughput

Time	Throughput Previous work	Throughput Enhanced Technique
0	0	0
3	0	0
6	0	1
9	0	0
12	0	11
15	0	40
18	35	82
19	94	124
23	94	138
27	94	138

Fig 4 shows that the packet drop ratio is less in proposed GA based method. But at some point of time it is same as in previous method. It means this enhanced scheme somewhere affects the performance with time.

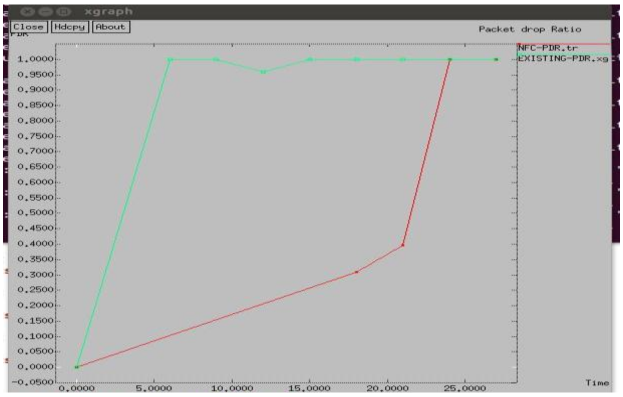

Fig 4: Packet Drop Ratio

Table 2: Packet Drop Ratio

Time	Packet drop ratio Previous work	Packet drop ratio Enhanced Technique
0	0	0
4	1	0.09
7	1	.15
10	.95	.19
14	1	.24
18	1	.28
20	1	.37
23	1	1
28	1	1

The major issue which is the main focus of this work is to reduce the storage requirement when TSM stores the generated pseudonyms and this objective is successively achieved by using Genetic algorithm. Fig 5 clears that the storage requirement gets decreased while implementing GA algorithm in the multiple pseudonym based method in conditional privacy preserving protocol.

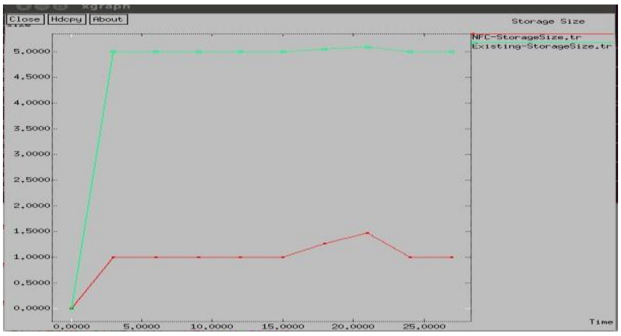

Fig 5: Storage Size

Table 3: Storage size

Time (sec)	Storage size (kb) Previous work	Storage size (kb) Enhanced Technique
0	0	0
3	5	1
6	5	1
9	5	1
13	5	1
15	5	1
18	5.1	1.3
21	5.2	1.5
24	5.1	1
27	5	1

5. CONCLUSION & FUTURE SCOPE

In the proposed system a new technique is generated at time of storing pseudonyms by TSM that is Genetic Algorithm to reduce the storage requirement of multiple pseudonyms based method in conditional privacy preserving protocol. Condition privacy preserving protocol developed is an optimized method for secure communication with NFC structure with multiple pseudonym based method and provide conditional PDU for further privacy of personal communication of the user for providing pseudonyms, which are essential for maintaining secure identification of the user, could be very useful in avoiding man in middle attack. Multiple pseudonym assigned by Trusted Service Manager is big advantage but lacks in storing, processing and communication cost. In this network environment is generated and then implement conditional privacy preserving protocol and to optimize GA is implemented on the CPP protocol. This proposed method reduces storage requirement as well as Delay and Packet Drop Ratio, & has increases the throughput on the generated network.

6. REFERENCES

[1] Wikipedia, "Near field communication", http://en.wikipedia.org/wiki/Near_field_ communication, Last accessed on 29 January, 2014.

[2] J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.

[3] ISO/IEC 18092, "Information technology: Telecommunications and information exchange between systems", Near field Communication Interface and Protocol (NFCIP-1), ISO/IEC, April 2004.

[4] Ernst Haselsteiner, "Security in Near Field Communication", Proceedings of the ACM Networking Conference, pp.14-18, December 2010

[5] Hasoo Eun, "Conditional Privacy Preserving Security Protocol for NFC Applications", IEEE Transactions on Consumer Electronics, Vol.59, No.1,pp.128-134, February 2013.

[6] Roy Want, "Near Field Communication", Published by the IEEE, Vol.16, No.9, pp.28-29, September 2011.

[7] Jeffrey Fischer, "NFC in Cell Phones: The New Paradigm for an Interactive World", Foundations and Trends in IEEE Communications Magazine, No.1–2, June, 2009.

[8] Florian Michahelles, "Pervasive RFID and Near Field Communication Technology", Published by the IEEE Computer Society, Vol.33, No.1, pp.34-39, Jan 2017.

[9] Eric Krevice Prebys," The Genetic Algorithm in Computer Science", MIT Undergraduate Journal of Mathematics,2002.

[10] Ali Alzahrani, Abdullah Alqhtani, Haytham Elmiligi, Fayez Gebali, Mohamed S. Yasein. "NFC security analysis and vulnerabilities in healthcare applications," IEEE Pacific Rim Conference on Computers and Signal Processing (PACRIM), 2013.

[11] Sheikh Gouse, Rhitul Kumbhar, "Network Simulation with TCL Script Generator for NS-2", International Journal of Emerging Trends in Science & Technology, Volume 01, Issue 06, pp.-827-829, 2014.

[12] M. Isaivani, and T. Sivasankari, "An Enhancement of Security Standards based on Pseudonyms in Near Field Communication", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Issue 3, pp.-2353-2357, 2014.