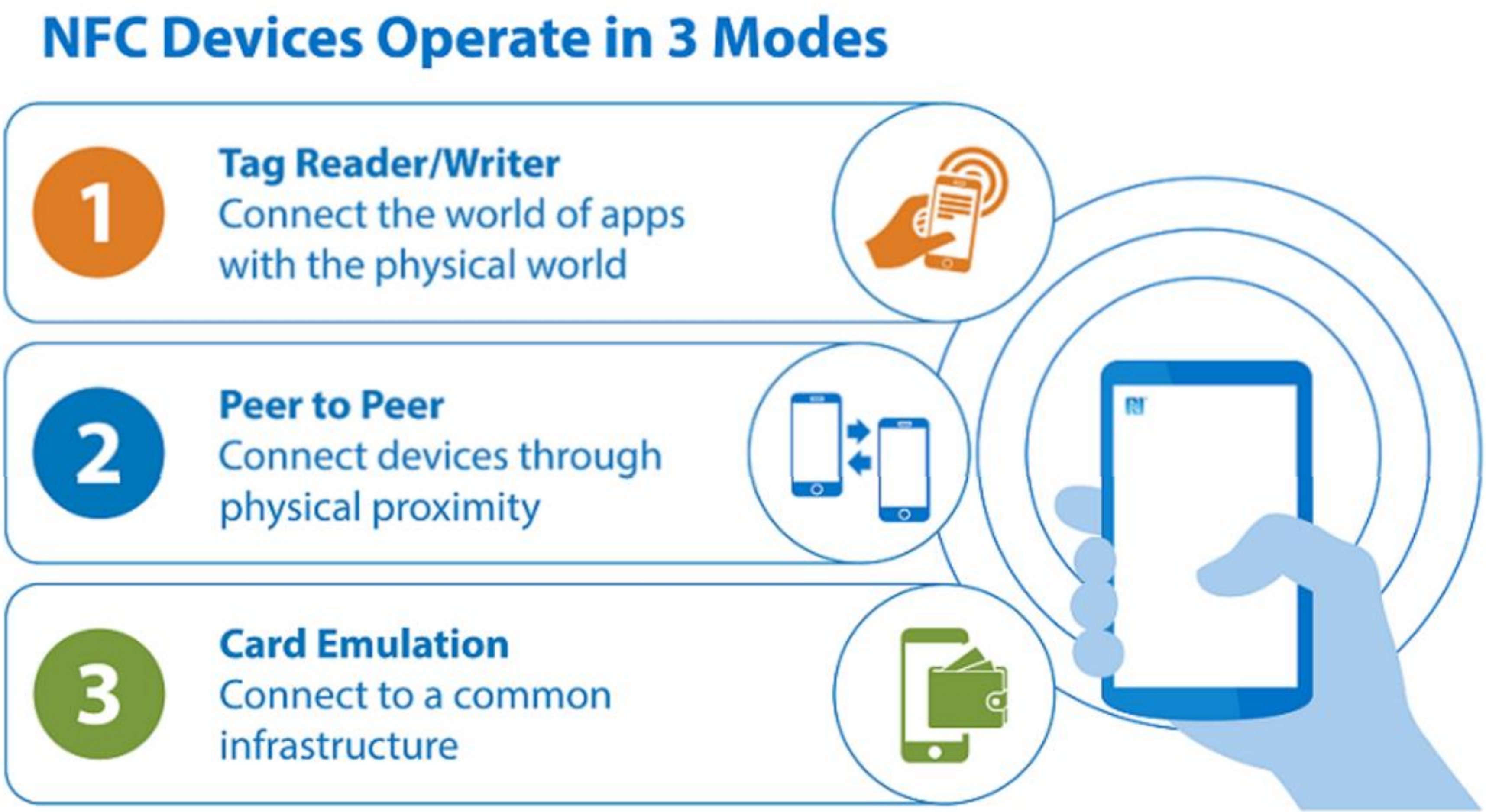
Analysis of Security Features and Threats to NFC systems

- *Chandini Shetty & Kiran Kumar G*

NFC Primer

- NFC has short communication range (usually 4 -10 cm), due to decaying magnetic induction between the antennas of NFC transmitter and receiver
- Favored by many security-sensitive applications, such as contactless payment due to guaranteed physical protection
- NFC communication process involves an initiator and a target
- Active and Passive Modes based on type of initator/Target
- ASK/PSK modulation schemes used to support data rates-106 kpbs, 212 kbps and 424 kbps
- Communication begins with initiator sending out discovery messages periodically- target respond to the probe
- Parameters exchanged to learn each other's capabilities before real data communication

Modes of Operation



Pic courtesy NFC-Forum.org

Applications of NFC Based Tags & Readers

NFC Architecture & Protocols- Security available by design

- RFCA- RF based collision avoidance protocol

  -The initiator senses the medium continuously at predefined intervals to avoid collision

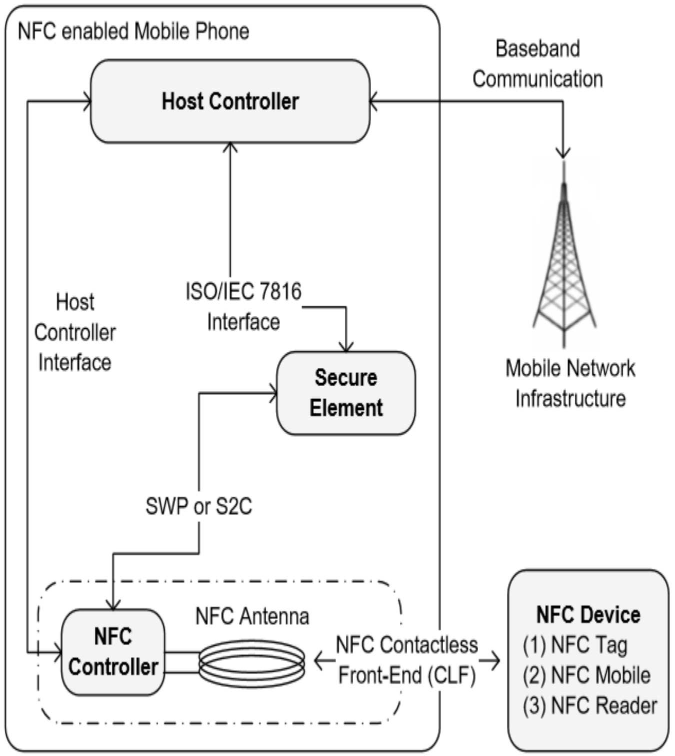
  -Begins transmission only when no nearby RF field

  This is an important deterrent to MITM attacks

- Device detection- Polling is done by initiator by broadcasting request packets to which targets can reply
- NFC-SEC : Cryptographic Mechanisms

  -Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement

  -Advanced Encryption Standard (AES) algorithm for data encryption and integrity



Possible Security threats on NFC communication enabled devices

- Eavesdropping
- Relay attacks
- Tag-based attacks
  - Spoofing/ Url Redirection for Malicious downloads
- Privacy Protection of user data

nShield:A Noninvasive NFC Security System for Mobile Devices

- Paper challenges the general perception that NFC is immune to eavesdropping attacks
- Able to eavesdrop from distance of 2.5m through experimental study with a portable NFC sniffer

What is nShield ?

  - an accessory security hardware attached to back of the phone

- Uses an adaptive attenuation algorithm which through a SDR controls the transmission power.
- Exploits the NFC target discovery process, to determines the right attenuation level for sustaining reliable data communication

*Ruogu Zhou, Guoliang Xing, Michigan State University, MobiSys 2014

Operation details:

- nShield charges only when the screen of the device is unlocked
  - the minimum harvested power depends on users interaction with mobile devices.
- If discharging level of the onboard battery is low, nShield automatically activates tag emulation, can charge itself rapidly
- Tag emulation mode : nShield starts responding to probing request from the initiator
  - Might interrupt with actual NFC use

  Solution to this:

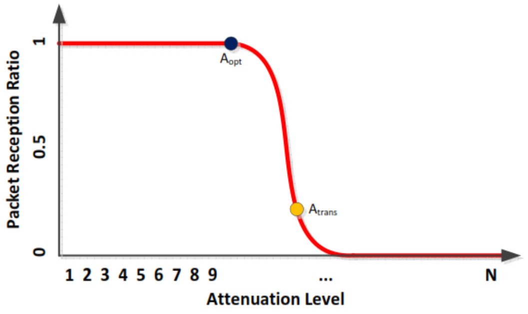
  - Pause 1sec after 2sec of charging, allowing initiator to proceed with discovery
  - Only if harvested power drops below 30%

Adaptive RF Field Attenuation Algorithm:

- Goal is to find optimal attenuation level amongst N levels

Challenge:

- To find A_{opt} without prior knowledge of target device, since depends on characteristics of target & distance
- Initiator attempts a polling request with attenuated field strength



- nShield infers if polling was successful based on whether SDD request follows from initiator
- If initiator waits for a certain period after the first polling request(typically to charge a tag) , then infers target is a tag
  - Algorithm uses 3 successful rounds of polling to select the attenuation level

Algorithm 6.1 *Adaptive RF Field Attenuation*

Input: N: number of attenuation levels.
Output: n_{opt}: optimal attenuation level.
Used sub-function: $Comm(n_i)$: attempt communication with attenuation level n_i. This sub-function returns "success" only if the first three polling rounds are completed successfully with the attenuation level n_i

$N_{upper} = N$
$N_{lower} = 1$
$n_{opt} = N/2$
while $N_{upper} - N_{lower} > 2$ **do**
    if $Comm(n_{opt}) = success$ **then**
        $N_{upper} = round((N_{upper} + n_{opt})/2)$
    else
        $N_{lower} = n_{opt}$
    end if
    $n_{opt} = round((N_{upper} + N_{lower})/2)$
end while
return n_{opt}

Results

- What is the maximum attenuation possible without compromising data transmission quality?
- What is resulting passive eavesdropping distance?

- Sniffer can achieve a maximum passive eavesdropping distance of around 80 cm
  - 67% (NFC Breakboard),48% (Neuxs 7), 39% (Note 2), and 31% (Galaxy Nexus) shorter than those without attenuation
- Optimal attenuation level varies significantly for different initiators
  - the NFC signal needs to be attenuated by 9.8 dB (NFC Breakboard), 5.9 dB (Neuxs 7), 4.2 dB (Note 2), and 2.2 dB (Galaxy Nexus), respectively
  - significant diversity is due to differences in initiator implementations Ex:size of antenna.

Security Analysis of NFC Relay Attacks using Probabilistic Model Checking

- Fast Communication channel is enabled between to distant victim NFC-enabled devices to carry out a relay attack
- Can bypass NFC short range requirements
- Authors demonstrate it is cheap and easy to carry out this attack
  - Leverages absence of localization evidence in NFC protocol
- Paper proposes a probabilistic model to study NFC protocol's resilience against relay attacks
  - PRISM Model checker is used to build the model
- Shows that NFC can be configured to thwart a relay attack
- Evaluates probability of relay attacks for range of channel characteristics that adversary should use

*Nikolaos Alexiou ; KTH Royal Inst. of Technol., Stockholm, Sweden ; Stylianos Basagiannis ; Sophia Petridou,
2014 International Wireless Communications and Mobile Computing Conference (IWCMC)

Setup of a relay attack

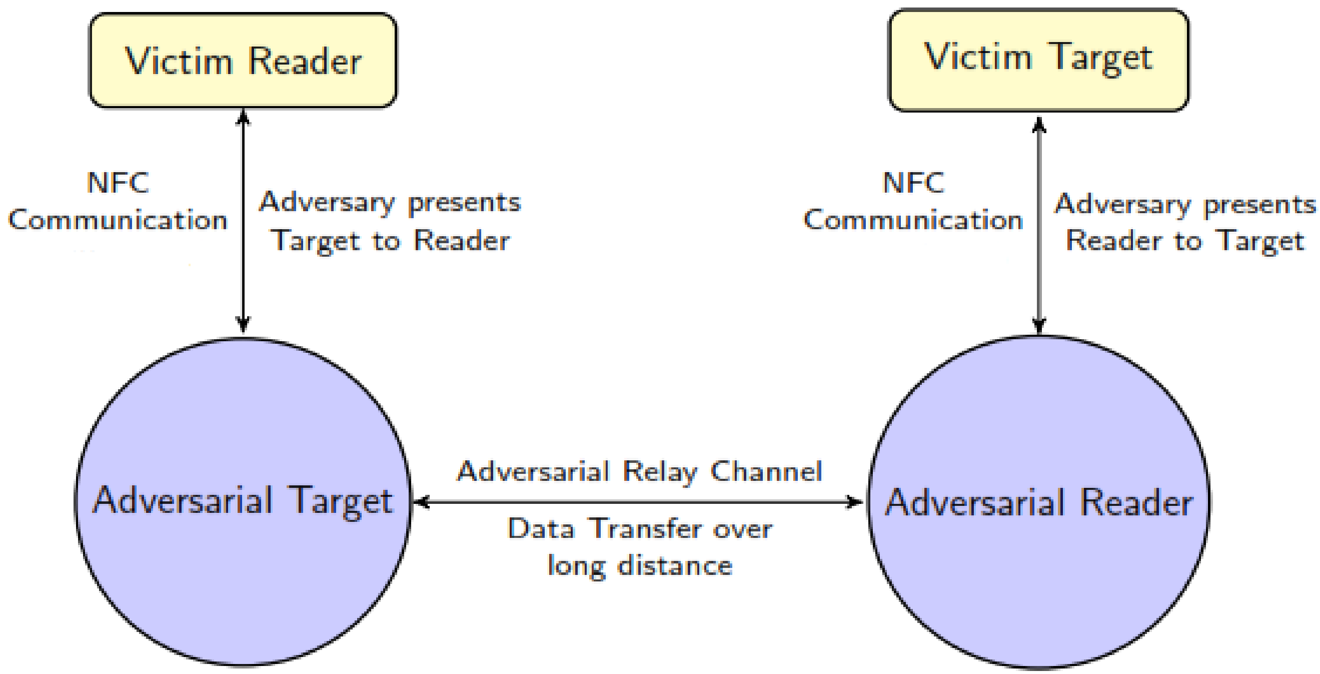


Figure 1. NFC Relay Attack Setup

PRISM Model

- Using PRISM a relay attack is modeled
- Four modules- one per device
- Model checking parameters are defined

Table II. MODEL CHECKING PARAMETERS

Parameter	Description
MAX_RWT	Timeout during data transport protocol
$PKTER$	Packet error rate of relay channel
DR_RCH	Relay channel data rate
DR_NFC	NFC data rate of 212 $kbps$
$NFCER$	Packet error rate of NFC
del	Time delays

- Properties that influence the probability of an attack
  - Timeouts during transport protocol
  - Adversarial strength in terms of relay channel data rate kbps
  - Adversarial channel quality
  - Size of data transmitted

- Model is configurable and realistic- additional delays can be accounted in the global parameter for delay

Results from the Model analysis:

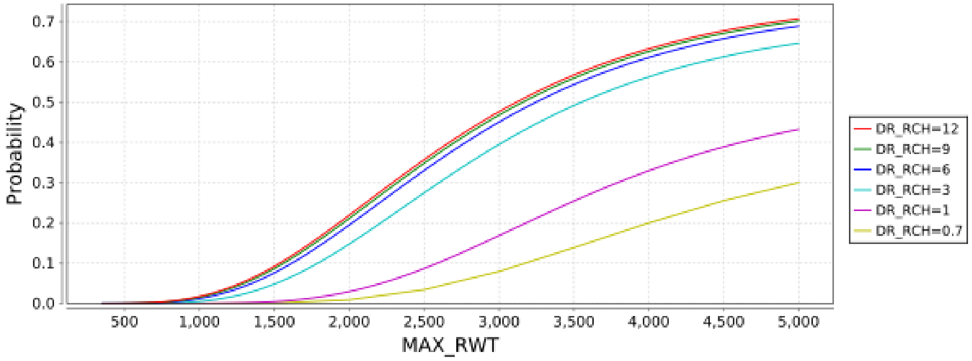


Figure 2. Relay Channel Rate vs Probability of Successful attack vs Timeout; low-data volume

- Strong adversaries (DR_RCH > 3Mbps) have a higher probability of performing a successful relay attack, which is above 60% for MAX_RWT > 4.5 sec
- Even weaker adversaries with slower relay channels (DR_RCH = 0:7; 1 Mbps) exhibit a very high probability of successfully launching the relay attack when MAX_RWT is high
- steep increase in the probability for higher DR_RCH and a slower increase for less powerful adversaries
  - Expected since powerful adversaries can take advantage of slight increasesin MAX_RWT values

Adversarial successfulness decreases rapidly when MAX_RWT is very low. For MAX_RWT < 1.5 sec & DR_RCH = 0:7 and 1 Mbps, very less probability of attack.

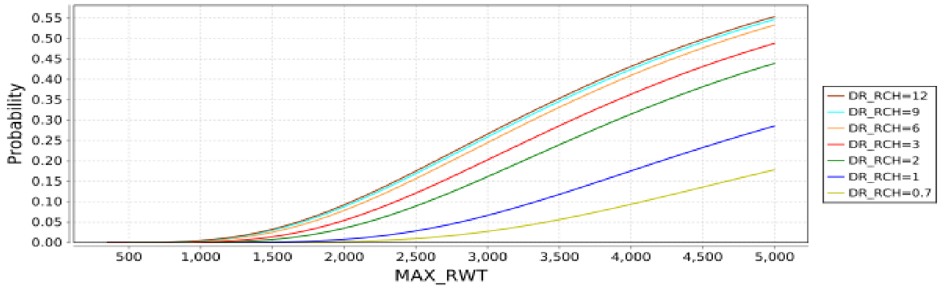


Figure 3. Relay Channel Rate vs Probability of Successful attack vs Timeout; high-data volume

- Increased volume of data that should be relayed poses an additional challenge for all adversarial strengths
- Only the most powerful of the adversaries (DR_RCH = 9; 12 Mbps) have a comparable success probability
- Performance of weaker adversaries is even worse

Conclusion: experimental setups show that stricter timeout values for MAX_RWT reduce the probability of an adversary to successfully launch a relay attack

Conditional Privacy Preserving Security Protocol for NFC Applications

- Some NFC applications are privacy sensitive- contactless payments
- User data can be collected from communication history to create a user profile- Resulting in loss of privacy
- Paper looks at vulnerabilities in the NFC-SEC key agreement protocol
- NFC standard requires key agreement for secret communication
- NFC-Sec Protocol standard requires the use of ECDH for key agreement protocol
- Users should exchange public key-received from CA

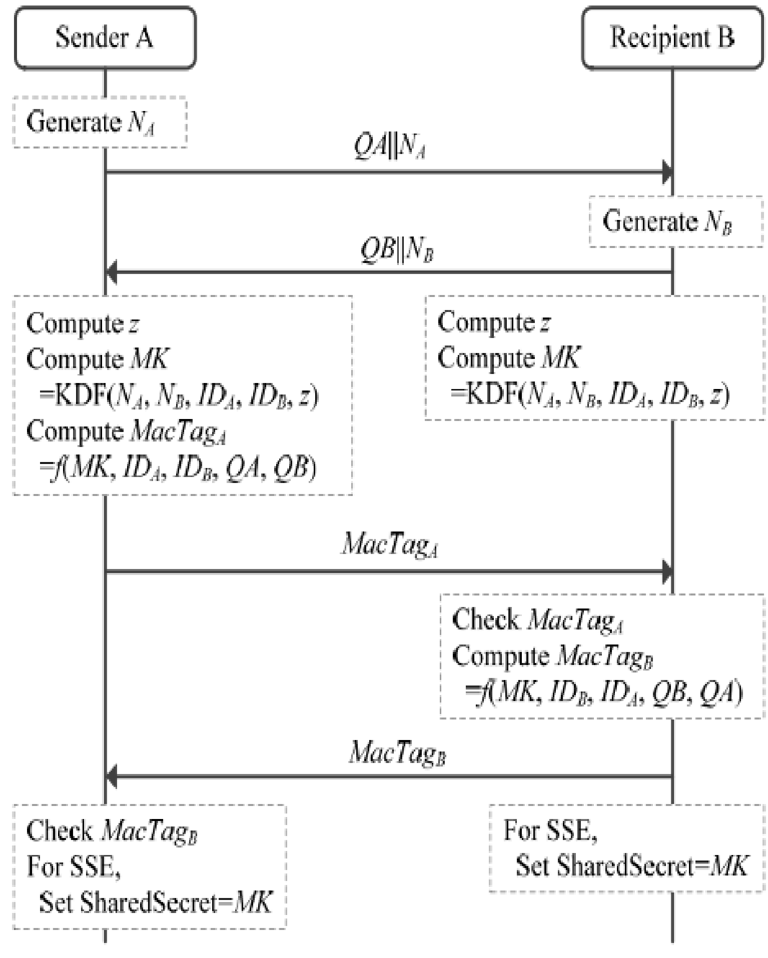
Proposes privacy protection methods based on pseudonyms to protect privacy of users

- Pseudonyms represents ID that changes randomly
- Composed of public key, private key, and a certificate & issued by a TTP

*Hasoo Eun, Hoonjung Lee and Heekuck Oh, KAIST, Korea, IEEE Transactions on Consumer Electronics, Vol. 59, No. 1, February 2013

Key agreement protocol of NFC

- NFC terminal must have public key and private key based on Elliptic curve
- SCH makes three keys hierarchically by using the key generated through SSE



Proposed solution by the paper

uPM: Self-updateable pseudonym based method

- NFC protocol is configured to update pseudonym without the need to communicate with TSM or use predefined set
- Q_A', Q_A'' are pseudonyms generated
- User B also cannot link that Q_A and Q_A' are with same entity

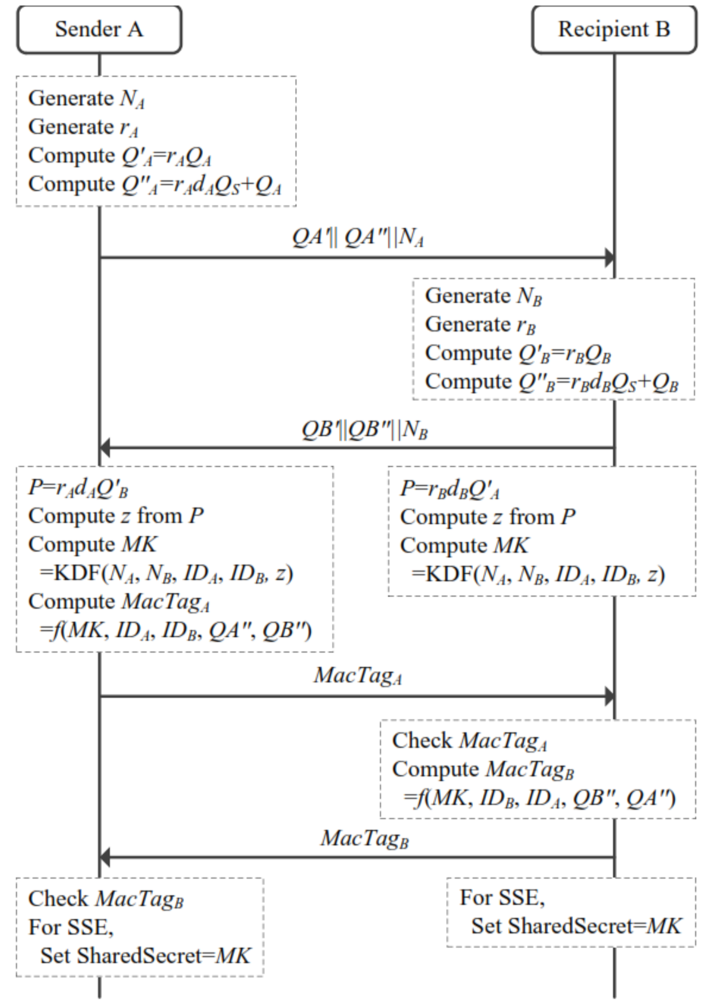


Figure 2. Proposed key agreement and confirmation protocol using self-updatable pseudonym based method

Security in Alternative NFC solutions that achieve NFC

- **VINCE:Exploiting visible light sensing for smartphone-based NFC systems**

- **Dhwani**
  - Enables NFC-like capability on the existing base of mobile phones
  - Acoustics-based NFC system that uses the microphone and speakers on mobile phones, eliminate need for specialized NFC hardware
  - Novel JamSecure technique, which uses self-jamming coupled with self-interference cancellation at the receiver
  - Provides an information-theoretically secure communication channel between the devices
  - Dhwani achieves data rates of up to 2.4 Kbps, which is sufficient for most existing NFC applications

VINCE:Exploiting visible light sensing for smartphone-based NFC systems

- Based on visible light spectrums (400THz to 790THz).
- VLC can offer short-range but secure and interference-free wireless links
- VINCE encodes information as different light intensities and displays on the smartphone screen
- Lights sensors on the receiver decodes by sensing the light signal
- Distance needs to be very short and direction can be controlled unlike RF
- No need for authentication
  - But NFC readers will be required to have light sensors

Challenges: Low data rate & unreliable transmissions

- Low refresh rate(60Hz) and variations in maximum refresh rate
- Interference from ambient light

*Jianwei Niu, Beihang Univ., Beijing, China,Fei Gu ; Ruogu Zhou ; Guoliang Xing ; Wei Xiang, MSU
INFOCOM2015

Solution to the VLC challenges

- VINCE employs a signal conditioner that detects outliers and uses an empirically derived model to compensate the received light samples
- Decoded data is verified using CRC (Cyclic Redundancy Check)
- If CRC fails, inform the sender via a feedback channel for retransmission
- Feedback channel is composed of an LED on the receiver and a light sensor on the smartphone.
- The feedback channel also enables rate-adaptation to maximize the system throughput
- Rate adaption scheme:
  - receiver measures the SNR of the current light channel
  - informs the sender to dynamically select the optimalencoding brightness levels.
- analytical model that characterizes the distance, SNR, and bit error rate of which guides the selection of transmission rate based on the measured reception SNR.