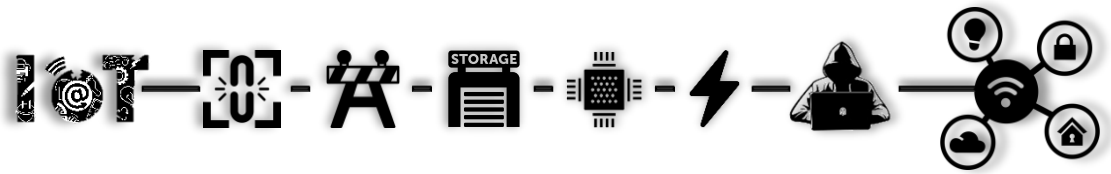
경희대학교
KYUNG HEE UNIVERSITY

Zero-Interaction Pairing and Authentication Using Moms Secret and Contextual Co-presence of Devices



PhD Public Defense Presentation

Oct 11th, 2022

Ubaid Ur Rehman
Dept. of Computer Science and Engineering,
Kyung Hee University, Republic of Korea

Advisors:
Professor Sungyoung Lee
Professor Seong-Bae Park

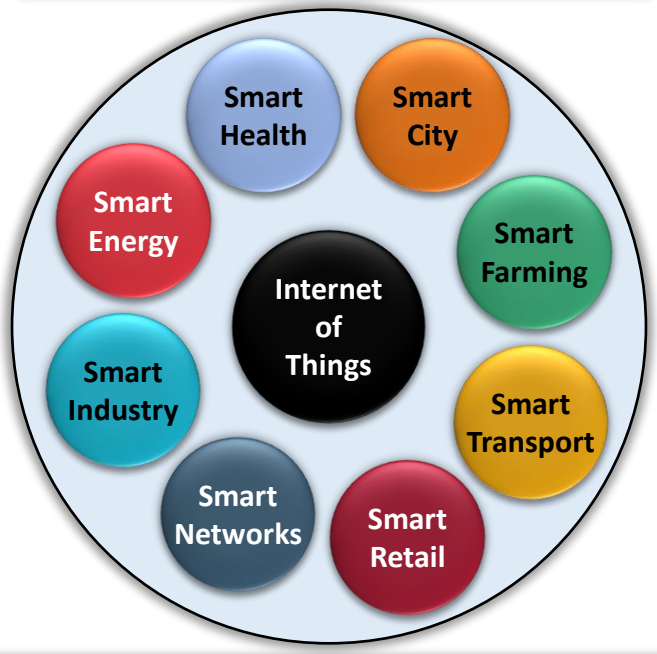
UCL Ubiquitous Computing Laboratory
Kyung Hee University, Korea

Agenda

- **INTRODUCTION**
  - Background
  - Motivation
  - Problem Statement
  - Research Taxonomy
- **RELATED WORK**
  - Literature Review
- **PROPOSED APPROACH**
  - Overview
  - Methodology
  - Concept Mapping
- **EVALUATION**
  - Experiment setup
  - Results Analysis
- **CONCLUSION**

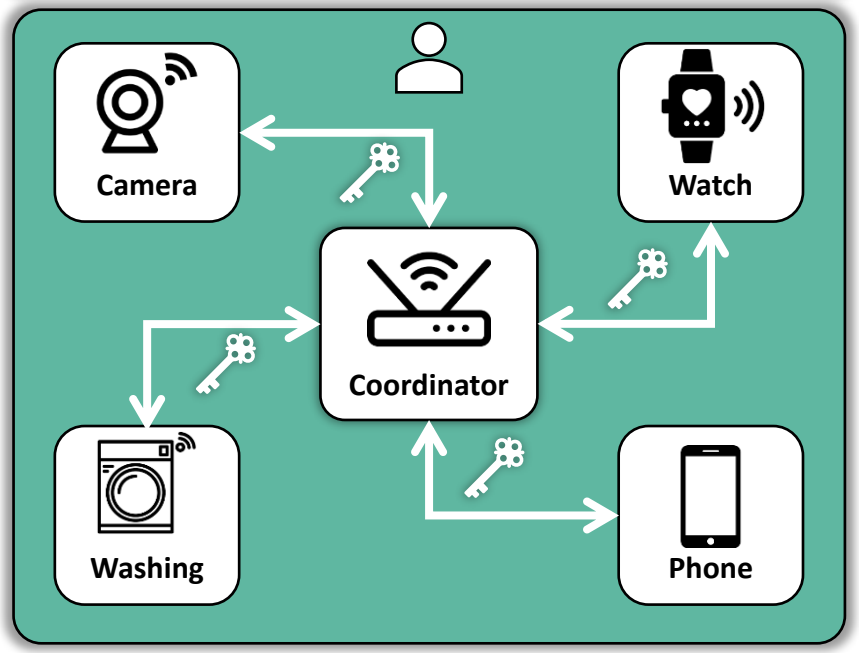
Background

Proliferation of Smart Devices



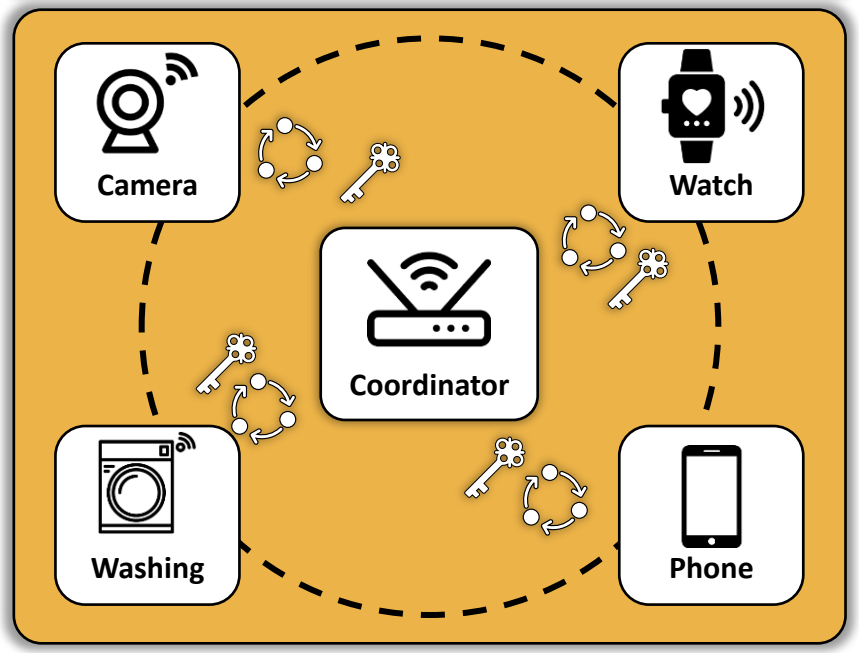
- **Internet of Things (IoT)** has been involved in **many domains** and equipped **humans with wearables and sensors** [1].
- Lead to the **development**, **personalized services**, and **improves lifestyle**.

User Assistance Pairing and Authentication



- Connections are secured by **pre-defined password** [2~4].
- **High user effort** during initial authentication procedure

Zero-Interaction Pairing and Authentication



- **Zero-involvement of user**, **periodic update**, and **dynamic password** [5~7].
- **Range** decides **acceptance or rejection** of devices

[Paula2017] Paula F. L., "Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios", Sociocybernetics, 2017.

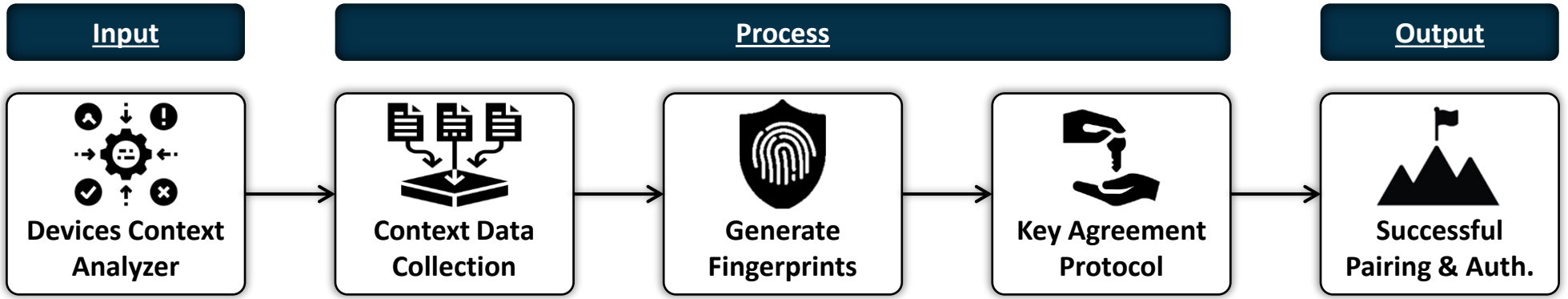
Motivation

IoT Devices

Characteristics [8~10]
- Low **Power**
- Low **Memory**
- Low **Computation**
- Limited **Battery Life**

Limitations [8~10]
- **User assistance pairing can not be deployed directly**
- Lack of **user interface**

ZERO-INTERACTION PAIRING AND AUTHENTICATION (ZIPA)



ZIPA – STRENGTHS [11~14]
- **Autonomous** pairing and authentication
- Pair the device **without any prior association** or **intermediate node**

ZIPA – Existing Schemes Limitations [11~14]
- **Prolong pairing time** to establish a shared key
- Vulnerable to **predictive contextual attack**

Problem Statement

Problem Statement

Zero Interaction Pairing and Authentication (ZIPA) uses **device physical context** that have **low entropy**, which leads to **predictive contextual attacks** [17]. Therefore, **sufficient contextual data** is required to provide **adequate security**, which results in **prolong pairing time** [11,14]. Moreover, the **existing user assistance pairing** is also vulnerable to the **key transportation attacks** [18,19].

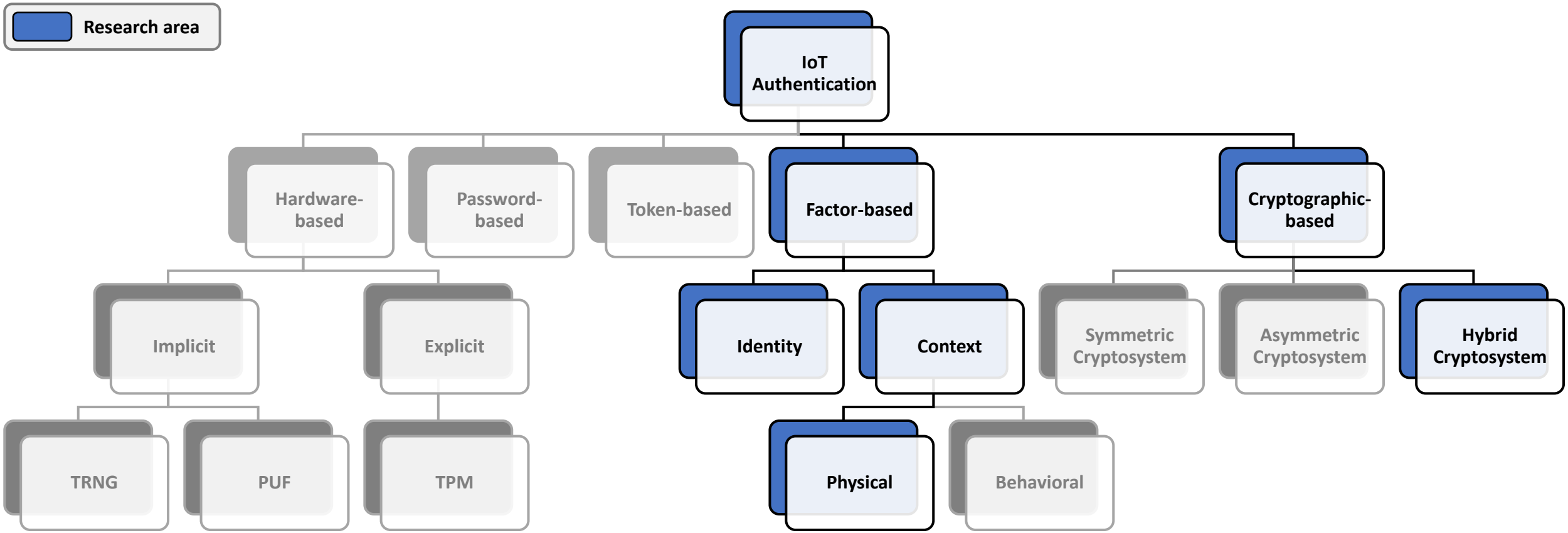
Goal

To design an **efficient ZIPA mechanism** that **reduces the pairing time** and ensure **strong resistance against predictive contextual** and **key transportation attacks**.

Challenges

- **C1** Utilization of **low entropy contextual data** for pairing and authentication [17]
- **C2** Use of **default global trusted center link key** for transportation of network key [18,19]
- **C3** **Verification of neighboring device** based on contextual copresence data [11,14]

Research Taxonomy



[Attkan2022] Attkan, Ankit, and Virender Ranga. "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security." *Complex & Intelligent Systems* (2022): 1-33.
[Nandy2019] Nandy, Tarak, et al. "Review on security of Internet of Things authentication mechanism." *IEEE Access* 7 (2019): 151054-151089.
[El-Hajj2019] El-Hajj, Mohammed, et al. "A survey of internet of things (IoT) authentication schemes." *Sensors* 19.5 (2019): 1141.

TRNG: True Random Number Generator
PUF: Physical unclonable function
TPM: Trusted Platform Module

Related Work

Challenges	Studies	Methodology	Limitations
Low Entropy Contextual Data (One-shot)	[Ustundag2021]	❖ **Contextual data** from smart manufacturing environment ❖ Use the **device electricity consumption** as a dynamic credentials for HMAC	❖ Vulnerable to **asynchronous attack** and **Impersonation Attack** ❖ **Low Entropy** value are used as key
	[Cabuk2021]	❖ Context-aware **mutual authentication** for proving the identity of a single or a group of drones that request to join the swarm ❖ The **mission ID** was considered as a context	❖ The proposed approach uses RSA and AES, which added **computation overhead** on each node.
Transportation of Network Key (Zero-Effort)	[Wang2020]	❖ Propose **certificate-less protocol** that leverage low-cost public key primitives ❖ Integrate **elliptic curve Diffie Hellman exchange** into existing association request/response messages ❖ **Improve the security** of installation code by using public key encryption	❖ The **security** of the existing approach depends on the **credential** and its **transmission** over the communication channel. ❖ The **credentials** are normally **global** and **publicly available** to all the users.
	[Li2020]	❖ **Analyze** the existing protocol using the security verification tool ❖ Presents the **insecurity** in the underlying **communication protocol stacks**	❖ The security analysis was performed based on **one attacking model**
Verification Of Neighboring Device (Co-presence)	[Fomichev2021]	❖ Proposed FastZIP that **reduces the pairing time** and provide **prevention** against the **contextual co-presence attacks** ❖ Adopt the **fuzzy password authentication key exchange protocol** for secure key agreement	❖ Fuzzy password authentication key exchange protocol enables **secure key agreement**, if the **two secret are close enough**
	[Fomichev2019]	❖ Address the **challenge of schemes** that do not reflect the realistic IoT scenarios ❖ **Comparative schemes** under the realistic conditions ❖ Collect and **release billion of sensors reading**	❖ **Fuzzy commitment** was used that **allows deviation** in the **fingerprint bits**

1# Low Entropy Contextual Data – Limitations

- Use **cryptographic hash** for **authentication**
- Use **low entropy** value that are **easily predictable**
- **Require time synchronization**

2# Transportation of Network Key – Limitations

- **Security** depends on the **credentials**
- **Credentials** are **global** and **publicly available**

3# Verification of Neighboring Device – Limitations

- Require **sufficient contextual data** for adequate security, leads to **prolong pairing time**
- Use **error correction method** for **fingerprint bits**

Zero-Interaction Pairing and Authentication
Proposed Methodology – Overview

- **Median of Medians (Moms)** secret generation for improved randomness and prevent information leakage

Contextual Data

Physical Context

Virtual Context

Solution 1: One-shot Pairing & Authentication
- Retrieve Contextual Data
- Pairing Devices Data
- Generate Moms Secret
- Moms Secret
- Zero-Knowledge Proof

Solution 2: Zero Effort Authentication & Pairing
- Mutual Authentication
- Authenticated Devices
- Key Provisioning
- Shared Symmetric Key
- Key Confirmation

- **Evolution of existing protocol** with self signed identifier and integrated encryption scheme

Ambient Context

Ambient Context

Solution 3: Co-presence-based Pairing & Authentication
- Generate Moms Secret
- Moms Secret
- Password Authenticated Key Exchange
- Shared Symmetric Key
- Trust Score Assignment

Pairing & Auth. Status

Succeed **Failed**

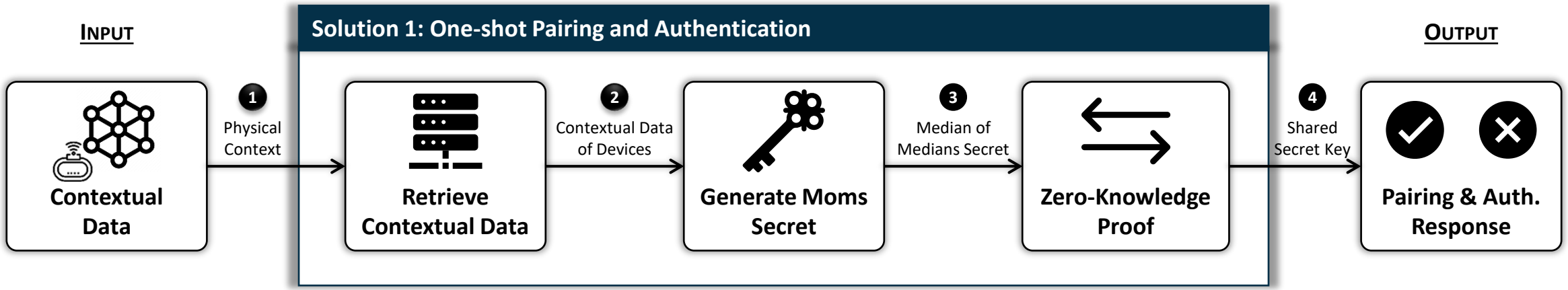
Pairing & Authentication Response

Patents Registration (2)
- 1 Registered **1** Domestic Patent
- 1 Applied **1** Domestic Patent

- **Pairing Time Reduction** & Resistance against contextual co-presence attack using Moms PAKE

Research Papers (5)
- 2 Published 2 Journals Papers
- 3 Published 3 Conferences Papers

Zero-Interaction Pairing and Authentication
Solution 1 – One-shot Pairing and Authentication



Contributions

- Use **interval based contextual data** that is **independent of time synchronization**
- Convert **low entropy value to high entropy** for **low information gain**
- **Median of medians (Moms) secret** generation improved **randomness** and **prevent information leakage**

Benefits

- Use **context-aware dynamic credential** for **one-shot device pairing & authentication**
- **Keys are refresh** upon **every authentication**
- **Independent** of **time synchronization**

[Rehman2021] **Rehman, Ubaid Ur**, Seong-Bae Park, and Sungyoung Lee. "Secure health fog: A novel framework for personalized recommendations based on adaptive model tuning." IEEE Access 9 (2021): 108373-108391.
[Rehman2019] **Rehman, Ubaid Ur,** and Sungyoung Lee. "Natural Language Voice based Authentication Mechanism for Smartphones." Proceedings of the 17th annual international conference on mobile systems, applications, and services (MobiSys). 2019.

Solution 1 – One-shot Pairing and Authentication

1# Retrieve Contextual Data and Generate Median of Medians Secret

Algorithm 1-1 : Median of Medians Secret Key Generation

Input: $C_{t_1}, ..., C_{t_n}$
Output: $M_{oms_{secret}}$

/* Retrieve Contextual Data */
1 $d_{C_x} \leftarrow Collect(C_{t_1}, ..., C_{t_n})$
/* Compute the Median of d_{C_x} */
2 $f_{MedVal} \leftarrow median(d_{C_x})$
3 $G_{f_{upper}} \leftarrow d_{C_x}[f_{MedVal} > d_{C_x}]$
4 $G_{f_{lower}} \leftarrow d_{C_x}[f_{MedVal} < d_{C_x}]$
/* Compute the Median of $G_{f_{upper}}$ */
5 $s_{MedVal} \leftarrow median(G_{f_{upper}})$
6 $G_{s_{upper}} \leftarrow G_{f_{upper}}[s_{MedVal} \geq G_{f_{upper}}]$
/* Compute the Median of $G_{f_{lower}}$ */
7 $t_{MedVal} \leftarrow median(G_{f_{lower}})$
8 $G_{t_{lower}} \leftarrow G_{f_{lower}}[t_{MedVal} \leq G_{f_{lower}}]$
9 $G_{1bits}, G_{2bits} \leftarrow int(G_{s_{upper}}), int(G_{t_{lower}})$
10 $G_{concat} \leftarrow G_{1bits} || G_{2bits}$
11 $P_{adBits} \leftarrow len(G_{concat})\%8$ /* for bytes */
12 $P_{adBits} \leftarrow 8 - P_{adBits}$ /* Padding Bits */
13 **if** $P_{adBits} \neq 0$ **then**
14 | $G_{Pad} \leftarrow Add\ P_{adBits}\ padding\ to\ G_{concat}$
15 **end**
16 **else**
17 | $G_{Pad} \leftarrow G_{concat}$
18 **end**
19 $B_{itsChunk} \leftarrow$ shape G_{Pad} into $8 - bits\ chunk$
20 $M_{oms_{secret}} \leftarrow int(B_{itsChunk}, 2)$

Time Complexity
$\mathcal{O}(n)$

1# Collect Contextual Data for Each Device
- **Timestamp || Power**

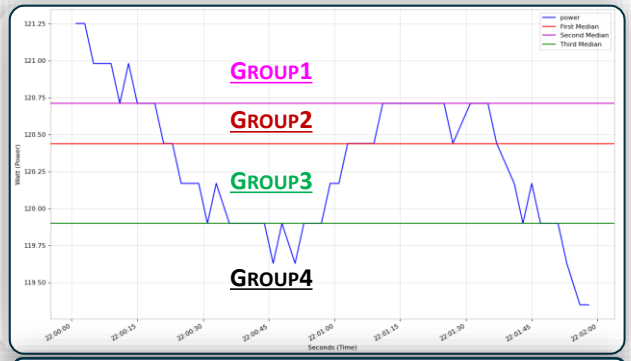
2# Compute the Median of Medians (Moms)
- **Low entropy** value to **high entropy** values
- **1st Median: Selected Contextual Interval**
- **2nd Median: Upper** than **1st Median**
- **3rd Median: Lower** than **1st Median**

3# Context Value to Bits based on Moms
- **Compare Group1 & 2** with **2nd Median value**
- **Compare Group 3 & 4** with **3rd Median value**

* Set value to zero's and one's

4# Padding, Shaping, & Key Generation
- Add **padding** for **byte conversion**
- **Split** the padded data into **8-bit chunks**
- **Convert** each **8-bit chunk to decimal value**

Contextual Interval: 60 seconds



[0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]

Generated Moms Secret

0401250011600012100

UCL KYUNG HEE UNIVERSITY

Solution 1 – One-shot Pairing and Authentication
2# Zero-Knowledge Proof

Algorithm 1-2 Zero-Knowledge Proof

Input: $D_{Moms_{secret}}, EC_M, EC_N$
Output: $D_1S_{hared_{secretKey}}, D_2S_{hared_{secretKey}}$

/* D_1 Preparation */
$r_{d1} \leftarrow$ selects random number $r_{d1} : 0 < r_{d1} < p$
$X_{d1} \leftarrow r_{d1} \cdot G$ /* G is a point on Elliptic Curve */
$T_{d1} \leftarrow D_{Moms_{secret}} \cdot EC_M + X_{d1}$
D_1 share T_{d1} with D_2
/* D_2 Preparation */
$r_{d2} \leftarrow$ selects random number $r_{d2} : 0 < r_{d2} < p$
$Y_{d2} \leftarrow r_{d2} \cdot G$ /* G is a point on Elliptic Curve */
$S_{d2} \leftarrow D_{Moms_{secret}} \cdot EC_N + Y_{d2}$
D_2 share S_{d2} with D_1
/* D_1 Compute $S_{hared_{secretKey}}$ */
$D_1S_{hared_{secretKey}} \leftarrow r_{d1} \cdot (S_{d2} - D_{Moms_{secret}} \cdot EC_N)$
$D_1S_{hared_{secretKey}} \leftarrow r_{d1} \cdot (D_{Moms_{secret}} \cdot EC_N + Y_{d2} - D_{Moms_{secret}} \cdot EC_N)$
$D_1S_{hared_{secretKey}} \leftarrow r_{d1} \cdot Y_{d2}$
$D_1S_{hared_{secretKey}} \leftarrow r_{d1} \cdot r_{d2} \cdot G$
/* D_2 Compute $S_{hared_{secretKey}}$ */
$D_2S_{hared_{secretKey}} \leftarrow r_{d2} \cdot (T_{d1} - D_{Moms_{secret}} \cdot EC_M)$
$D_2S_{hared_{secretKey}} \leftarrow r_{d2} \cdot (D_{Moms_{secret}} \cdot EC_M + X_{d1} - D_{Moms_{secret}} \cdot EC_M)$
$D_2S_{hared_{secretKey}} \leftarrow r_{d2} \cdot X_{d1}$
$D_2S_{hared_{secretKey}} \leftarrow r_{d2} \cdot r_{d1} \cdot G$
$D_2S_{hared_{secretKey}} \leftarrow r_{d1} \cdot r_{d2} \cdot G$
if $D_1S_{hared_{secretKey}} == D_2S_{hared_{secretKey}}$ **then**
  $A_{uthStatus} \leftarrow Succeed$
end
else
  $A_{uthStatus} \leftarrow Failed$
end

TIME COMPLEXITY $\mathcal{O}(1)$

5# Zero-Knowledge Proof

- Use the **Zero Knowledge Proofs** with **Elliptic curve cryptography**
  - Provide **128bits security**
- **M** & **N** are **point generation seed**
- **G** is a **group** of order ***p x h***
  - ***p*** is a **large prime number**
  - ***h*** is the **co-factor**

* Operation are conducted (*mod p*)

Device 1
- Select **random number** r_{d1} and G point on **EC**
- Compute T_{d1}

Device 2
- Select **random number** r_{d2} and G point on **EC**
- Compute S_{d2}

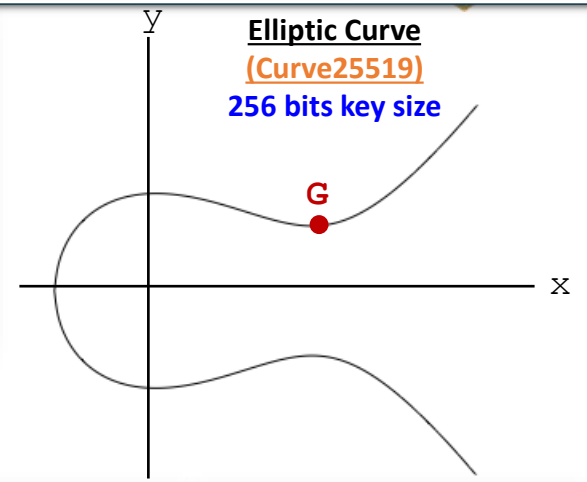
T_{d1}:
QSipN5vp3EzPOjH/NFf3fEIn
Zc90AAFn0zJzbGHR03Te

S_{d2}:
QlAxYPPUz1jNC2bNNC5CcL
ZFlorrKLXaPgTDL5Gb9mUo

T_{d1} S_{d2}

$S_{haredKey}$:
XfqLM8QFjUvSyiHYstjnJM9
pWa1RwXkX4g2vB3NZKd0=

$S_{haredKey}$:
XfqLM8QFjUvSyiHYstjnJM9
pWa1RwXkX4g2vB3NZKd0=



Elliptic Curve
(Curve25519)
256 bits key size

Solution 1: One-shot Pairing and Authentication

Device 1

$X = r_{d1} * G$
$T_{d1} = Moms_{Secret} * M + X$

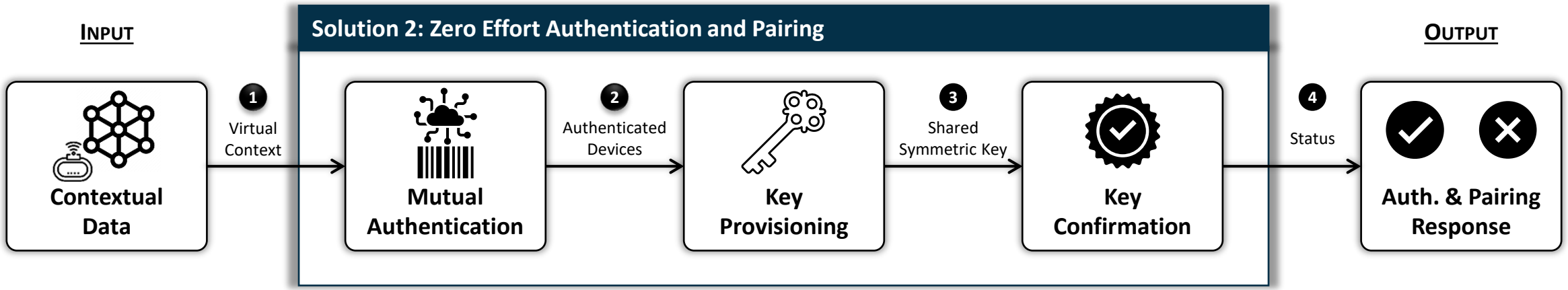
$S_{haredKey} = r_{d1} * (S_{d2} - Moms_{Secret} * N)$

Device 2

$Y = r_{d2} * G$
$S_{d2} = Moms_{Secret} * N + Y$

$S_{haredKey} = r_{d2} * (T_{d1} - Moms_{Secret} * M)$

Zero-Interaction Pairing and Authentication
Solution 2 – Zero-Effort Authentication and Pairing



Contributions

- **Identify** the **vulnerability of network key transportation** in user assistance pairing scheme
- **Mutual authentication** using **self signed identifier** instead of device identification only
- **Key provisioning** based on **integrated encryption scheme**

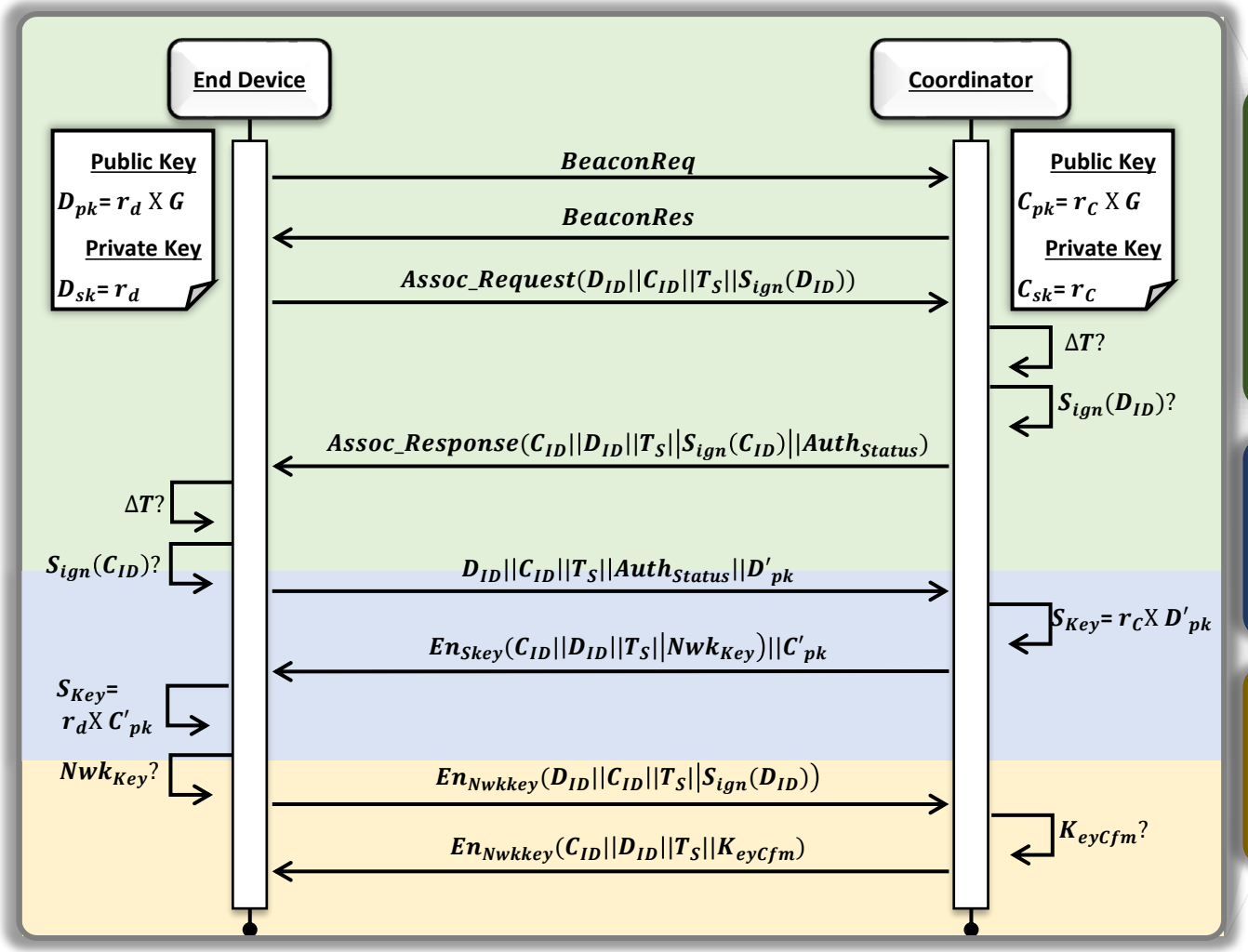
Benefits

- **Non-user assistance pairing scheme evolve the existing communication protocols**
- **Automate** the **joining process** of new device
- **Ensure resistance** against **masquerading**, **man-in-the-middle**, **key transportation**, and **replay attacks**

[Rehman2021] **Rehman, Ubaid Ur,** Seong-Bae Park, and Sungyoung Lee. "Secure health fog: A novel framework for personalized recommendations based on adaptive model tuning." IEEE Access 9 (2021): 108373-108391.
[Rehman2021] 이승룡, **Ubaid Ur Rehman**, 박성배, "An Intelligent Context-Sensitive Protocol Recommender System for Wireless Sensor Network", 출원번호: 10-2021-0188377, 2021.12.27 (출원인: 경희대학교 산학협력단)
[Rehman2019] **Rehman, Ubaid Ur,** and Sungyoung Lee. "TPP: Tradeoff Between Personalization and Privacy." International Conference on Ubiquitous Information Management and Communication. Springer, Cham, 2019.

Solution 2 – Zero-Effort Authentication and Pairing

Mutual Authentication, Key Provisioning, & Key Confirmation



1# Mutual Authentication

- **End device** create a **self-signed identifier** to **prove its identity**
- **ΔT** is an **estimated time delay** to ensure **resistance against replay attack**
- **Coordinator** also create a **self-signed identifier** to ensure **mutual authentication**

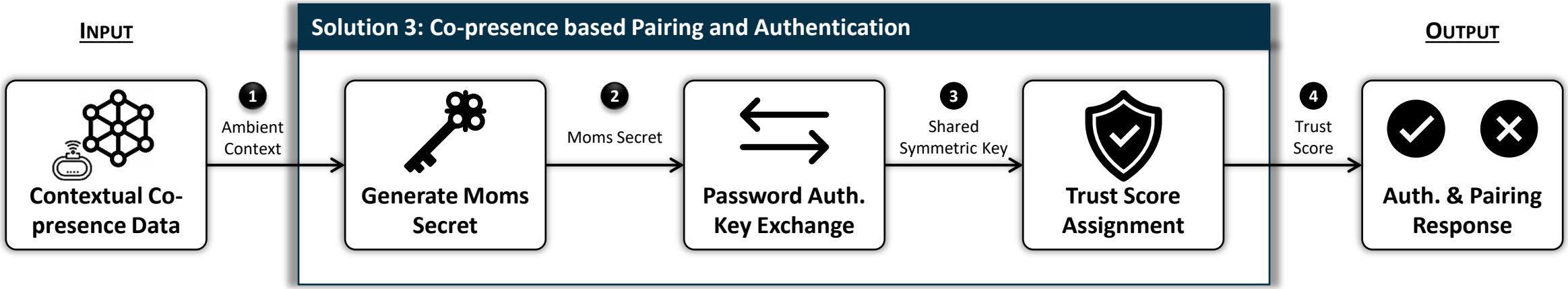
2# Key Provisioning

- **Coordinator** generate **shared key** using **end device public key** & securely **transmit the network key** along with **public key**.

3# Key Confirmation

- **End device** shared the **self-signed identifier**, **encrypted with network key** to ensure the **secure transportation of network key.**

Zero-Interaction Pairing and Authentication
Solution 3 – Co-presence based Pairing and Authentication



Contributions

- **Innovative design** by utilizing the **Moms Secret** and **Password Authenticated Key Exchange (PAKE)** to **reduce the pairing time** and **improve security**
- Assign the **trust score** to each pairing device based on **pairing attempt** and **success rate**

Benefits

- **Allow the pairing** between **co-presence devices only**
- Compute the **fingerprint of ambient context** sensed by the devices
- Ensure **resistance** against **predictable contextual attacks**

[Rehman2022] 이승룡, **레만 우바이드 유알**, "음성 이미지 기반 사용자 인증 장치 및 그 방법", 등록번호 : 10-2444003, 2022년09월15일 (특허권자:경희대학교 산학협력단)
[Rehman2022] **Rehman, Ubaid Ur**, et al. "A Novel Mutual Trust Evaluation Method for Identification of Trusted Devices in Smart Environment." 2022 16th International Conference on Ubiquitous Information Management and Communication. IEEE, 2022.

Zero-Interaction Pairing and Authentication
Solution 3 – Co-presence based Pairing and Authentication

Solution 3: Co-presence based Pairing and Authentication

Generate Moms Secret → Password Auth. Key Exchange → Trust Score Assignment

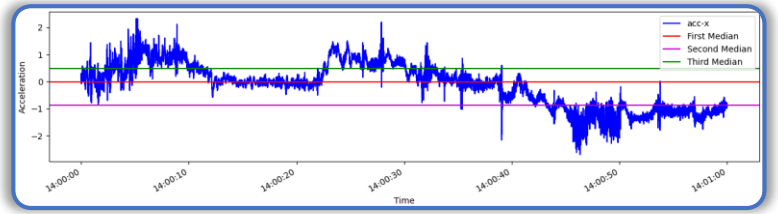
Algorithm 3-1 Co-presence based Pairing and Authentication

Input: Co-presence-based Modalities Data $M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}}$
Output: Authentication Status $A_{uthStatus}$

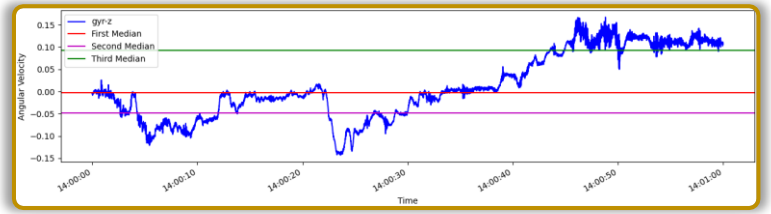
1 $\mathcal{M}_{Ctx} \leftarrow Load\ M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}}$
2 **foreach** $c \in \mathcal{M}_{Ctx}$ **do**
3 $M_{dims} \leftarrow dimension(c)$
4 **if** $M_{dims} > 1$ **then**
5 $M_{dic}(k_{ey}, v_{alue}) \leftarrow split(c, M_{dims})$
6 **for** $i\ in\ range(M_{dic})$ **do**
7 $D_{evMoms_{Secret}}[i] \leftarrow M_{omsSecret}(d)$
8 **end**
9 $D_{evMoms_{Secret}} \leftarrow Optimum_{Secret}(D_{evMoms_{Secret}})$
10 **end**
11 **else**
12 $D_{evMoms_{Secret}} \leftarrow M_{omsSecret}(c)$
13 **end**
14 $S_{electedMoms_{Secret}}.append(D_{evMoms_{Secret}})$
15 **end**
16 $D_{Shared_{Key}} \leftarrow PAKE(S_{electedMoms_{Secret}})$
17 **if** $D_{Shared_{Key}} == D'_{Shared_{Key}}$ **then**
18 $A_{uthStatus} \leftarrow Succeed$
19 $D_{T_{score}} \leftarrow Increment\ T_{score}$
20 $D'_{T_{score}} \leftarrow Increment\ T_{score}$
21 **end**
22 **else**
23 $A_{uthStatus} \leftarrow Failerd$
24 $D_{T_{score}} \leftarrow Decrement\ T_{score}$
25 $D'_{T_{score}} \leftarrow Decrement\ T_{score}$
26 **end**

Selected Data for Moms Secret Generation

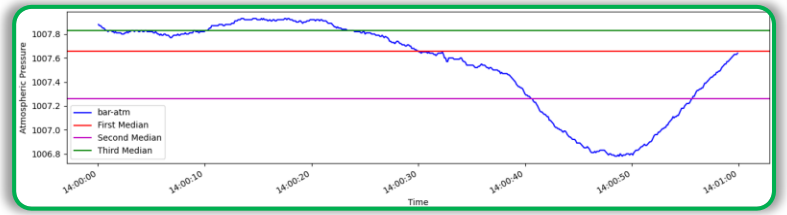
MODALITY# 01 (SELECTED DIMENSION)



MODALITY# 02 (SELECTED DIMENSION)



MODALITY# 03 (NO SELECTION)



- Generated Moms Secret = 960bits
- Window Size = 1 minutes
- Number of Instance = 3 x 6000
- Generated Moms Secret Security = 2^{480}
- Execution Time = 4.078 seconds

Shared Key Using Password Authenticated Key Exchange

- Shared Key Using PAKE = 256bits
- PAKE Execution Time = 0.0358 seconds
- Total Execution Time for Successful Pairing (3 Modalities) = 4.1138 seconds
- Trust Score (each) = 0.6

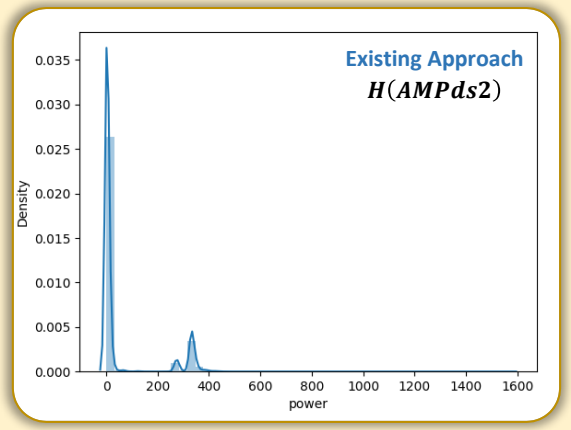
EVALUATIONS AND RESULTS

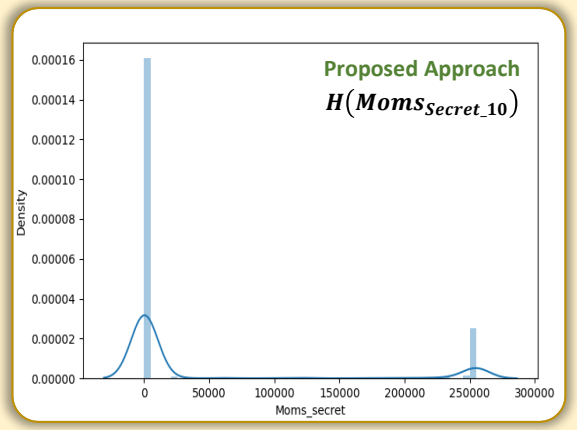
- ❖ **Entropy ∝ Randomness**
- ❖ **Entropy ∝ $\frac{1}{\text{Information Gain}}$**
- ❖ $H(X) = -\sum_{x \in X} p(x) log_2\, p(x)$

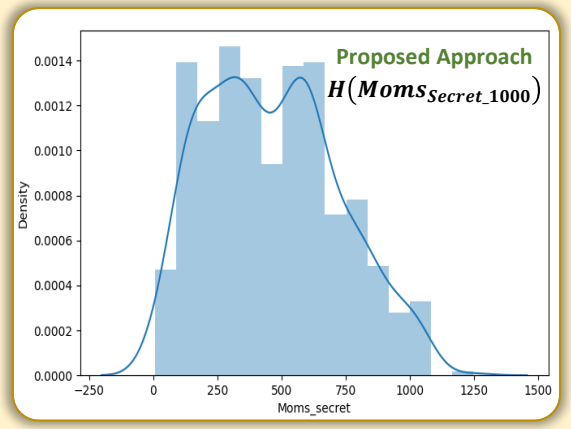
Solution 1 – One-shot Pairing and Authentication
1# Entropy Assessment

Dataset#1 – The Almanac of Minutely Power dataset (AMPds2) [22]

SHANNON ENTROPY ASSESSMENT







ENTROPY ASSESSMENT – FINDINGS

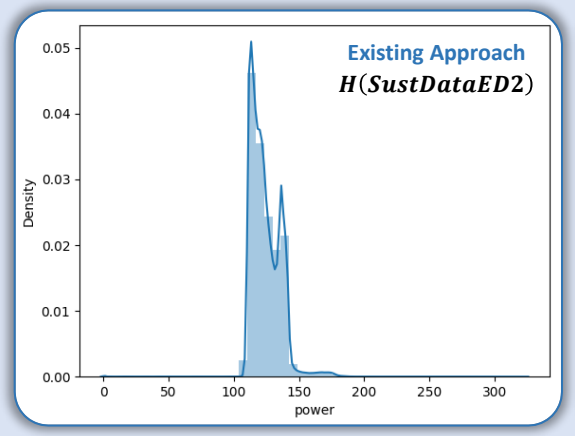
$$H(AMPds2) = 2.1693$$
$$H(Moms_{Secret\_10}) = 3.8805$$
$$H(Moms_{Secret\_1000}) = 4.8454$$

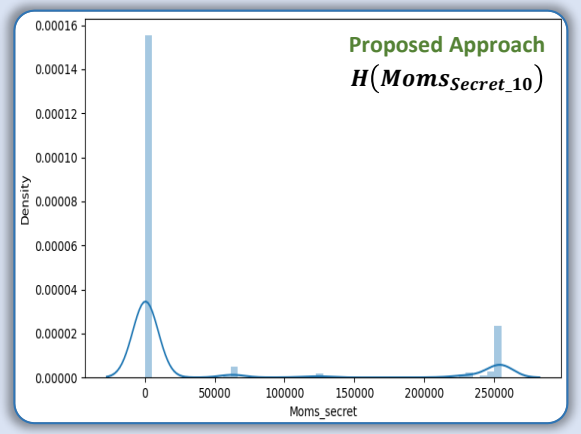
✅ $H(Moms_{Secret\_10}) > H(AMPds2)$

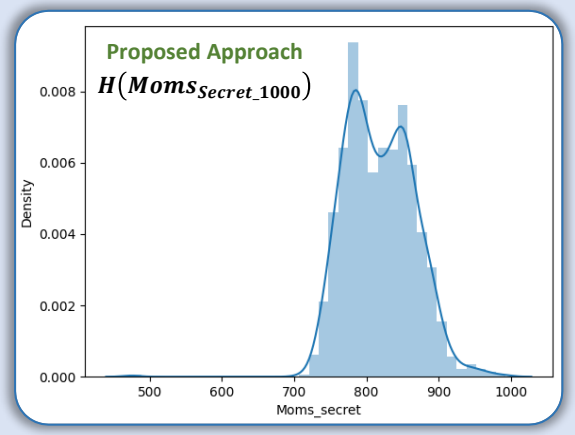
✅ $H(Moms_{Secret\_1000}) > H(AMPds2)$

Dataset#2 – Sustainable Data for Energy Disaggregation (SustDataED2) [23]

SHANNON ENTROPY ASSESSMENT







ENTROPY ASSESSMENT – FINDINGS

$$H(SustDataED2) = 3.1275$$
$$H(Moms_{Secret\_10}) = 3.8964$$
$$H(Moms_{Secret\_1000}) = 4.1728$$

✅ $H(Moms_{Secret\_10}) > H(SustDataED2)$

✅ $H(Moms_{Secret\_1000}) > H(SustDataED2)$

[Ustundag2021] Ustundag Soykan, Elif, et al. "Context-Aware Authentication with Dynamic Credentials using Electricity Consumption Data." *The Computer Journal* (2021).

Solution 1 – One-shot Pairing and Authentication
2# Probability of Guessing Contextual

Dataset#1 – The Almanac of Minutely Power dataset (AMPds2) [22]

Existing Approach

- $C_{MinValue} = 1$ — Minimum Value in Dataset
- $C_{MaxValue} = 1571$ — Maximum Value in Dataset
- $T_{count} = 157001$ — All possible values between min & max
- $T_{values} = 694456$ — Total values within dataset
- $p(C_{t\_D1}) = 9.1717 * 10^{-12}$ — Probability of Guessing Contextual value

Proposed Approach

- $T_{values} = 694456$ — Total values within dataset
- $M_{omWinSize} = 55$ — Instances in selected window size
- $L = 12$ — Length of generated Moms Secret
- $p(M_{omsSecVal}) = 0.0039$ — Probability of identifying 1 value
- $p(M_{omsSecVal\&Pos}) = 1.2621 * 10^{-29}$ — Probability of identifying 1 value at specific position
- $p(M_{omsSecret\_D1}) = 9.9962 * 10^{-34}$ — Probability of Guessing Contextual Pattern

Probability of Guessing Context – Findings

$p(M_{omsSecret\_D1}) < p(C_{t\_D1})$

Dataset#2 – Sustainable Data for Energy Disaggregation (SustDataED2) [23]

Existing Approach

- $C_{MinValue} = 0.38$ — Minimum Value in Dataset
- $C_{MaxValue} = 323.39$ — Maximum Value in Dataset
- $T_{count} = 32302$ — All possible values between min & max
- $T_{values} = 1048575$ — Total values within dataset
- $p(C_{t\_D2}) = 2.9523 * 10^{-11}$ — Probability of Guessing Contextual value

Proposed Approach

- $T_{values} = 1048575$ — Total values within dataset
- $M_{omWinSize} = 55$ — Instances in selected window size
- $L = 12$ — Length of generated Moms Secret
- $p(M_{omsSecVal}) = 0.0039$ — Probability of identifying 1 value
- $p(M_{omsSecVal\&Pos}) = 1.2621 * 10^{-29}$ — Probability of identifying 1 value at specific position
- $p(M_{omsSecret\_D2}) = 6.6203 * 10^{-34}$ — Probability of Guessing Contextual Pattern

Probability of Guessing Context – Findings

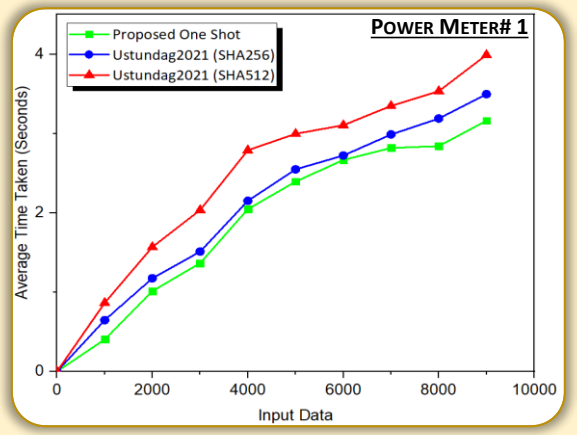
$p(M_{omsSecret\_D2}) < p(C_{t\_D2})$

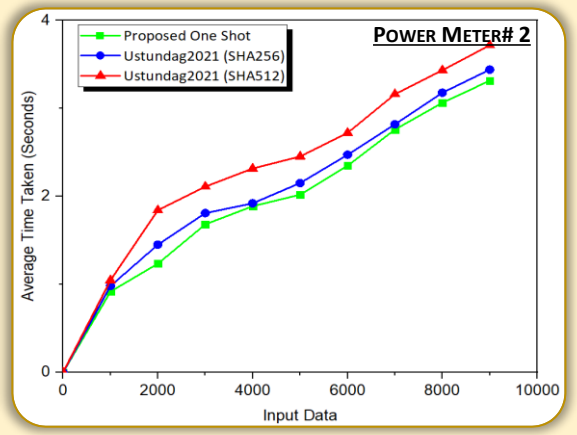
[Ustundag2021] Ustundag Soykan, Elif, et al. "Context-Aware Authentication with Dynamic Credentials using Electricity Consumption Data." *The Computer Journal* (2021).

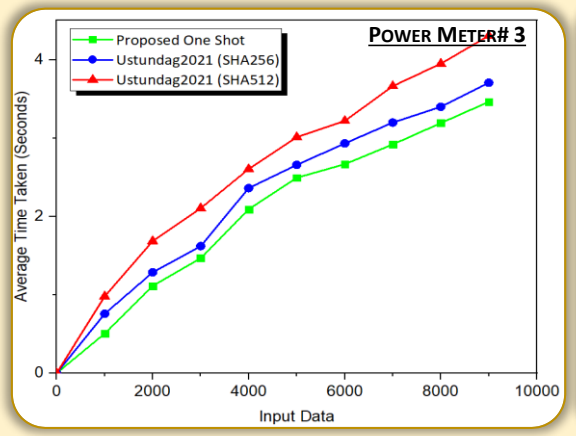
Solution 1 – One-shot Pairing and Authentication
3# Time Complexity

Time Complexity
- Secure Hash Algorithm (SHA):
  - $\mathcal{O}(c+xn)$
- Proposed OneShot:
  - $\mathcal{O}(n)$

Dataset#1 – The Almanac of Minutely Power dataset (AMPds2) [22]







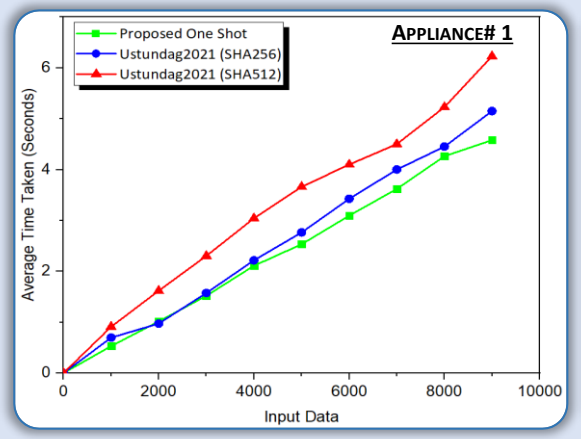
Time Complexity – Decreased

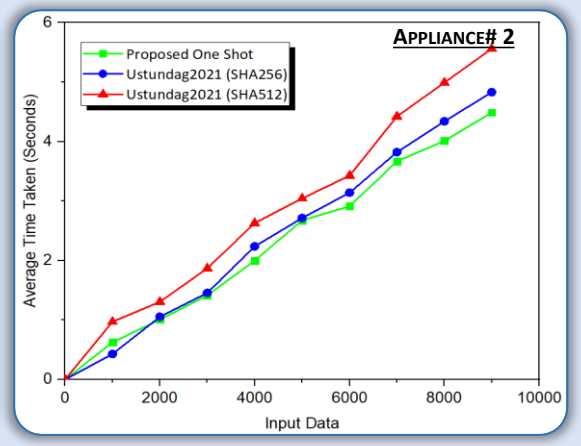
Power Meter# 1
- $OneShot\ vs\ SHA256 = 9.55\%$
- $OneShot\ vs\ SHA512 = 20.76\%$

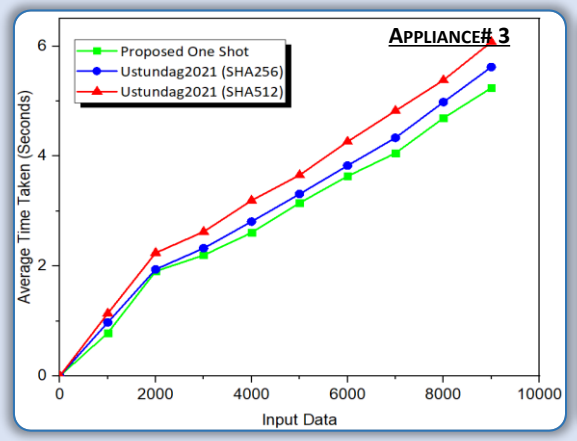
Power Meter# 2
- $OneShot\ vs\ SHA256 = 3.64\%$
- $OneShot\ vs\ SHA512 = 10.83\%$

Power Meter# 3
- $OneShot\ vs\ SHA256 = 6.58\%$
- $OneShot\ vs\ SHA512 = 19.59\%$

Dataset#2 – Sustainable Data for Energy Disaggregation (SustDataED2) [23]







Time Complexity – Decreased

Appliance# 1
- $OneShot\ vs\ SHA256 = 11.08\%$
- $OneShot\ vs\ SHA512 = 26.51\%$

Appliance# 2
- $OneShot\ vs\ SHA256 = 7.08\%$
- $OneShot\ vs\ SHA512 = 19.32\%$

Appliance# 3
- $OneShot\ vs\ SHA256 = 6.77\%$
- $OneShot\ vs\ SHA512 = 13.76\%$

[Ustundag2021] Ustundag Soykan, Elif, et al. "Context-Aware Authentication with Dynamic Credentials using Electricity Consumption Data." *The Computer Journal* (2021).

Solution 2 – Zero-Effort Authentication and Pairing

1# Security Analysis – Scyther & AVISPA Results

❖ **DOLEV AND YAO MODEL:**

- ❖ **Network** is assumed to be **under full control of the adversary**
- ❖ **Attacker** can **read**, **modify**, **delete**, and **inject messages** on the **communication channel**

1# SCYTHER – SECURITY ANALYSIS RESULTS

Scyther results : verify

Claim				Status		Comments
ZeroEffortAuthandPairing	EndDevices	ZeroEffortAuthandPairing,EndDevices1	Secret ScrtKey	Ok	Verified	No attacks.
SECRET		ZeroEffortAuthandPairing,EndDevices2	Secret NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevices3	Secret DataPkt	Ok	Verified	No attacks.
ALIVE		ZeroEffortAuthandPairing,EndDevices4	Alive	Ok	Verified	No attacks.
WEAKAGREE		ZeroEffortAuthandPairing,EndDevices5	Weakagree	Ok	Verified	No attacks.
COMMIT		ZeroEffortAuthandPairing,EndDevices6	Commit Coordinator,ScrtKey	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevices7	Commit Coordinator,NwkK	Ok	Verified	No attacks.
NIAGREE		ZeroEffortAuthandPairing,EndDevices8	Niagree	Ok	Verified	No attacks.
NISYNCH		ZeroEffortAuthandPairing,EndDevices9	Nisynch	Ok	Verified	No attacks.
	Coordinator	ZeroEffortAuthandPairing,Coordinator1	Secret ScrtKey	Ok	Verified	No attacks.
SECRET		ZeroEffortAuthandPairing,Coordinator2	Secret NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator3	Secret DataPkt	Ok	Verified	No attacks.
ALIVE		ZeroEffortAuthandPairing,Coordinator4	Alive	Ok	Verified	No attacks.
WEAKAGREE		ZeroEffortAuthandPairing,Coordinator5	Weakagree	Ok	Verified	No attacks.
COMMIT		ZeroEffortAuthandPairing,Coordinator6	Commit Coordinator,ScrtKey	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator7	Commit Coordinator,NwkK	Ok	Verified	No attacks.
NIAGREE		ZeroEffortAuthandPairing,Coordinator8	Niagree	Ok	Verified	No attacks.
NISYNCH		ZeroEffortAuthandPairing,Coordinator9	Nisynch	Ok	Verified	No attacks.

Done.

2# AVISPA – SECURITY ANALYSIS RESULTS

SPAN 1.6 - Protocol Verification : ZeroEffortAuthandPairing.hlpsl

File

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
/home/span/span/testsuite/results/ZeroEffortAuthandPairing.if

Save file | View CAS+ | View HLPSL | Protocol simulation | Intruder simulation | Attack simulation

Tools

HLPSL

HLPSL2IF

IF

Choose Tool option and press execute

Execute

OFMC | ATSE | SATMC | TA4SP

- ❖ **Secrecy**, **authentication**, **proof-of-origin**, and **integrity**
- ❖ **Bounded session verification & values are publicly available**
- ❖ **Model support intruder using algebraic properties and protocol falsification**

KG Elliptic Curve Key Pair Generation
GS Generation of Signature
VS Verification of Signature
SK Secret Key Generation
En Encryption
Dc Decryption
U User Association
GH Generation of Hash

Solution 2 – Zero-Effort Authentication and Pairing
2# Performance Evaluation

Existing Approach (Wang2020)

End Device

- $O_{perationOverhead} = K_G + G_S + G_H + S_K + E_n + D_c$
- $T_{imeOverhead} = 0.158134$ seconds
- $M_{emoryOverhead} = 259\ Bytes$

Coordinator

- $O_{perationOverhead} = K_G + G_H + V_S + S_K + E_n + D_c$
- $T_{imeOverhead} = 0.163121$ seconds
- $M_{emoryOverhead} = 195\ Bytes$

[Wang2020] Wang, Weicheng, et al. "Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy." *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2020.

Zero-Effort (Proposed)

End Device

- $O_{perationOverhead} = K_G + G_S + V_S + S_K + E_n + 2D_c$
- $T_{imeOverhead} = 0.025293$ seconds
- $M_{emoryOverhead} = 238\ Bytes$

Coordinator

- $O_{perationOverhead} = K_G + G_S + 2V_S + S_K + 2E_n + D_c$
- $T_{imeOverhead} = 0.027485$ seconds
- $M_{emoryOverhead} = 238\ Bytes$

[Rehman2021] Rehman, Ubaid Ur, Seong-Bae Park, and Sungyoung Lee. "Secure health fog: A novel framework for personalized recommendations based on adaptive model tuning." *IEEE Access* 9 (2021): 108373-108391.

Solution 3 – Co-presence based Pairing and Authentication
1# Dataset Selection & Similarity Identification

Evaluation Metrics

- **Similarity Pattern Identification (Ablation Study)**
  - Selection of **data dimension** for Moms Secret
  - Reduce **fingerprint generation overhead**
- **Comparison with State-of-the-Art**
  - **Reduction of Pairing Time**
  - Co-presence-based **Device Identification** and **Attack Resistance Rate**

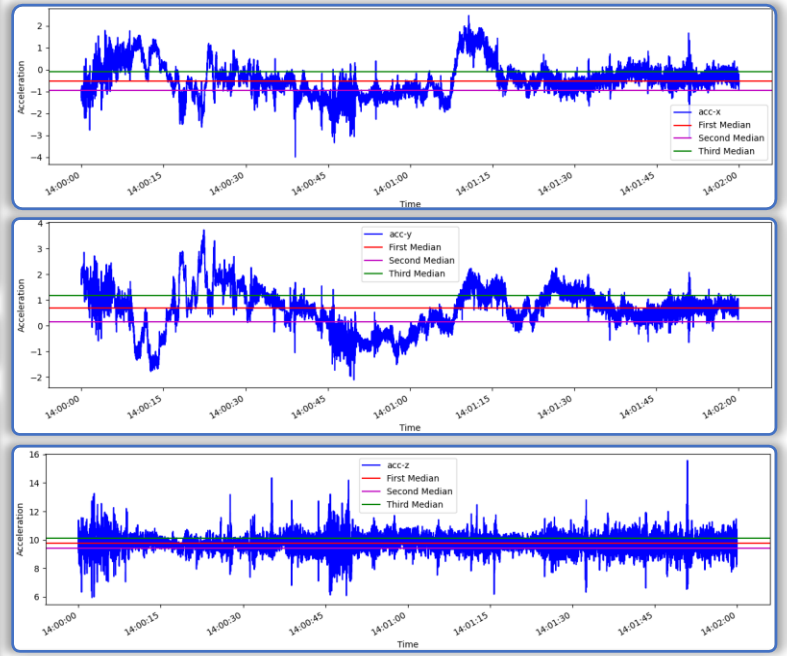
Dataset Selection

FastZip Dataset [11]

- Data collected using **6 smartphone**
  - Distributed **inside the vehicle**
  - Total **4 vehicles** are used (6 phone/vehicle)
  - **Adversarial & non-adversarial settings**
- **Features:**
  - Accelerometer
  - Gyroscope
  - Barometer

1# Similarity Pattern Identification – Moms Secret Generation

Accelerometer (x, y, z)

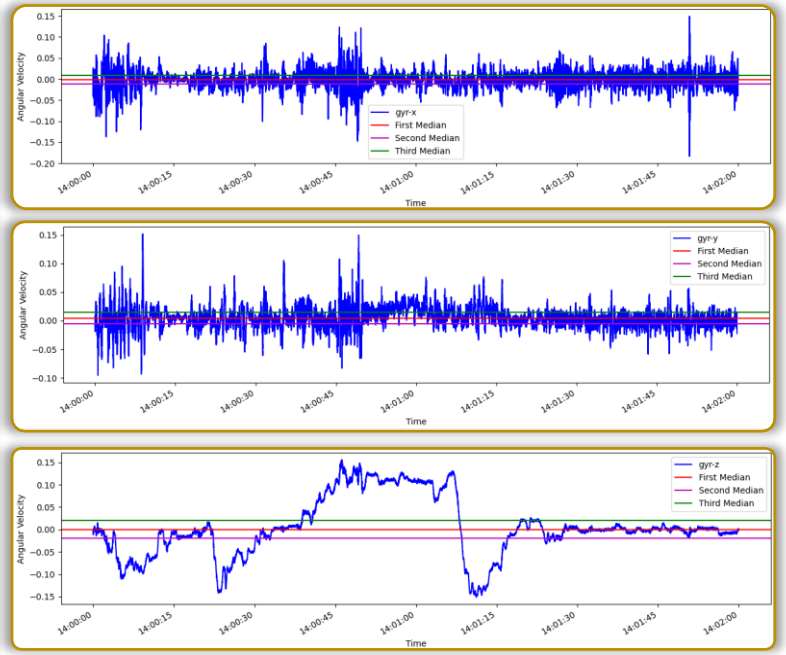


Findings

- **60.42%** similar bits between **x** and **y**
- **50.24%** similar bits between **x** and **z**
- **51.45%** similar bits between **y** and **z**

x

Gyroscope (x, y, z)



Findings

- **52.21%** similar bits between **x** and **y**
- **48.78%** similar bits between **x** and **z**
- **53.63%** similar bits between **y** and **z**

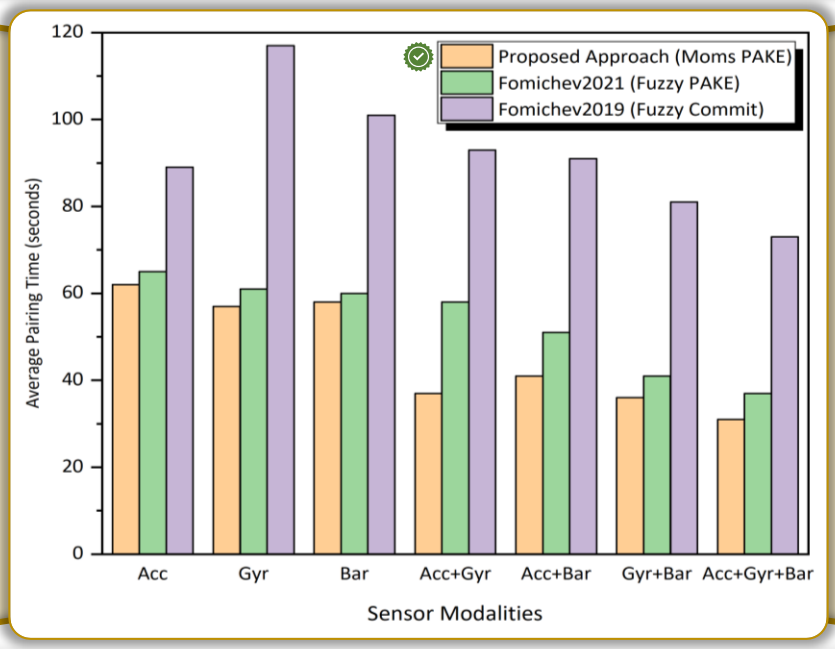
z

Solution 3 – Co-presence based Pairing and Authentication

2# Reduction of Pairing Time, Device Identification & Attack Resistance Rate

Comparison with the State-of-the-Art

1# Reduction of Pairing Time



Comparison	Acc	Gyr	Bar	Acc+Gyr	Acc+Bar	Gyr+Bar	Acc+Gyr+Bar
$Moms_{PAKE}$ *vs* $Fuzzy_{PAKE}$	4.62%	6.56%	3.33%	36.21%	19.61%	12.2%	16.22%
$Moms_{PAKE}$ *vs* $Fuzzy_{Commit}$	30.34%	51.28%	42.57%	60.22%	54.95%	55.56%	57.53%

2# Device Identification & Attack Resistance Rate

Co-presence based	$Moms_{PAKE}$	$Fuzzy_{PAKE}$	$Fuzzy_{Commit}$
Device Identification	93.04%	92.15%	91.37%
Attack Resistance Rate	96.91%	93.64%	79.19%

Low Attack Resistance Rate – Existing Approaches [11,14]

- Use **error correction mechanism** such as Reed-Solomon (RS) code that **detect** and **correct multiple symbol errors**.
  - Support the **adversary for guessing a specific context**

Findings

- **Reduction of pairing time** depends:
  - Number of **sensor's modalities**
  - Selection of **appropriate data for Moms Secret (Fusion)**

Conclusion

Thesis Contributions

One-shot Pairing & Authentication

- Use **interval based contextual data** that is **independent of time synchronization**
- Convert **low entropy value to high entropy** for **low information gain**
- **Median of medians (Moms) secret** generation improved **randomness** and **prevent information leakage**

Zero-Effort Authentication & Pairing

- Identify the **vulnerability of network key transportation** in **user assistance pairing scheme**
- **Mutual authentication** using **self signed identifier** and **integrated encryption scheme**

Co-presence-based Pairing & Authentication

- **Identify the neighboring device** based on **contextual co-presence data**
- **Reduce the pairing time** by using **sensor fusion and Moms secret**
- **Resistance against predictable contextual attacks**

Future Work

- **Moms Secret** with **integrated environmental sensors** measuring the **ambient characteristics**
- **Machine learning scheme for key generation** process in ZIPA scheme.
- **Blockchain based contextual co-presence pairing and authentication scheme** for constrained node network.

Achievements

Published Papers

- **SCI(E) Journals (05)**
  - First Author: 02 Published
  - Co-author: 03 Published
- **Domestic Journals (01)**
  - Co-Author: 01 Published
- **Conferences (08)**
  - First Author: 03 (International)
  - Co-Author: 01 (International)
  - First Author: 04 (Domestic)
- **Domestic Patents (01)**
  - Registered: 01

Publication

Total Publications (15)

First Author Publications (10)

특허증
CERTIFICATE OF PATENT

특 허 제 10-2444003 호
Patent Number

출원번호 제 10-2020-0165034 호
Application Number
출원일 2020년 11월 30일
Filing Date
등록일 2022년 09월 13일
Registration Date

발명의명칭 Title of the Invention
음성 이미지 기반 사용자 인증 장치 및 그 방법

특허권자 Patentee
경희대학교 산학협력단(134571-*******)
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

발명자 Inventor
등록사항란에 기재

위의 발명은 「특허법」에 따라 특허원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.

2022년 09월 13일

특허청
Korean Intellectual Property Office

특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE

References

1. **[Sadoughi2020]** Sadoughi, Farahnaz, Ali Behmanesh, and Nasrin Sayfouri. "Internet of things in medicine: a systematic mapping study." Journal of biomedical informatics 103 (2020): 103383.
2. **[Soriente2008]** Soriente, Claudio, Gene Tsudik, and Ersin Uzun. "HAPADEP: human-assisted pure audio device pairing." International Conference on Information Security. Springer, Berlin, Heidelberg, 2008.
3. **[Saxena2006]** Saxena, Nitesh, et al. "Secure device pairing based on a visual channel." 2006 IEEE Symposium on Security and Privacy (S&P'06). IEEE, 2006.
4. **[Ischi2009]** Ischi, Reto. Security properties of device pairing protocols. MS thesis. ETH, Swiss Federal Institute of Technology Zurich, Information Security Department, 2009.
5. **[Corner2002]** Corner, Mark D., and Brian D. Noble. "Zero-interaction authentication." Proceedings of the 8th annual international conference on Mobile computing and networking. 2002.
6. **[Miettinen2014]** Miettinen, Markus, et al. "Context-based zero-interaction pairing and key evolution for advanced personal devices." Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. 2014.
7. **[Truong2014]** Truong, Hien Thi Thu, et al. "Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication." 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, 2014.
8. **[Sehgal2012]** Sehgal, Anuj, et al. "Management of resource constrained devices in the internet of things." IEEE Communications Magazine 50.12 (2012): 144-149.
9. **[Kumar2006]** Kumar, Sandeep S. Elliptic curve cryptography for constrained devices. Diss. Bochum, Univ., Diss., 2006, 2006.
10. **[Pisani2020]** Pisani, Flávia, et al. "Fog computing on constrained devices: Paving the way for the future iot." Advances in Edge Computing: Massive Parallel Processing and Applications 35 (2020): 22-60.
11. **[Fomichev2021]** Fomichev, Mikhail, et al. "FastZIP: faster and more secure zero-interaction pairing." Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services. 2021. https://doi.org/10.5281/zenodo.4777836
12. **[Putrada2021]** Putrada, Aji Gautama, and Nur Ghaniaviyanto Ramadhan. "A Proposed Hidden Markov Model Method for Dynamic Device Pairing on Internet of Things End Devices." Journal of ICT Research & Applications 14.3 (2021).
13. **[Lee2021]** Lee, Kyuin, and Younghyun Kim. "Balancing Security and Usability of Zero-interaction Pairing and Authentication for the Internet-of-Things." Proceedings of the 2th Workshop on CPS&IoT Security and Privacy. 2021.
14. **[Fomichev2019]** Fomichev, Mikhail, et al. "Perils of zero-interaction security in the Internet of Things." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3.1 (2019): 1-27.
15. **[Lee2019]** Lee, Kyuin, et al. "Voltkey: Continuous secret key generation based on power line noise for zero-involvement pairing and authentication." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3.3 (2019): 1-26.
16. **[Fomichev2019]** Fomichev, Mikhail, Max Maass, and Matthias Hollick. "Zero-Interaction Security-Towards Sound Experimental Validation." GetMobile: Mobile Computing and Communications 23.2 (2019): 16-21.
17. **[Ustundag2021]** Ustundag Soykan, Elif, et al. "Context-Aware Authentication with Dynamic Credentials using Electricity Consumption Data." The Computer Journal (2021).
18. **[Wang2020]** Wang, Weicheng, et al. "Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy." Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2020.
19. **[Li2020]** Li, Li, Proyash Podder, and Endadul Hoque. "A formal security analysis of ZigBee (1.0 and 3.0)." Proceedings of the 7th Symposium on Hot Topics in the Science of Security. 2020.
20. **[Cabuk2021]** Cabuk, Umut Can, Gokhan Dalkilic, and Orhan Dagdeviren. "CoMAD: Context-aware mutual authentication protocol for drone networks." IEEE Access 9 (2021): 78400-78414.
21. **[Huang2021]** Huang, Huihui, et al. "An efficient ECC-based authentication scheme against clock asynchronous for spatial information network." *Mathematical Problems in Engineering* 2021 (2021).
22. **[Makonin2016]** Makonin, Stephen, 2016, "AMPds2: The Almanac of Minutely Power dataset (Version 2)", https://doi.org/10.7910/DVN/FIE0S4, Harvard Dataverse
23. **[Pereira2020]** Pereira, Lucas. 2020. “A Residential Labeled Dataset for Smart Meter Data Analytics.” OSF. March 20. doi:10.17605/OSF.IO/JCN2Q.

Thank you!

Comments & Suggestions