RAMA: Real-Time Automobile Mutual Authentication Protocol Using PUF

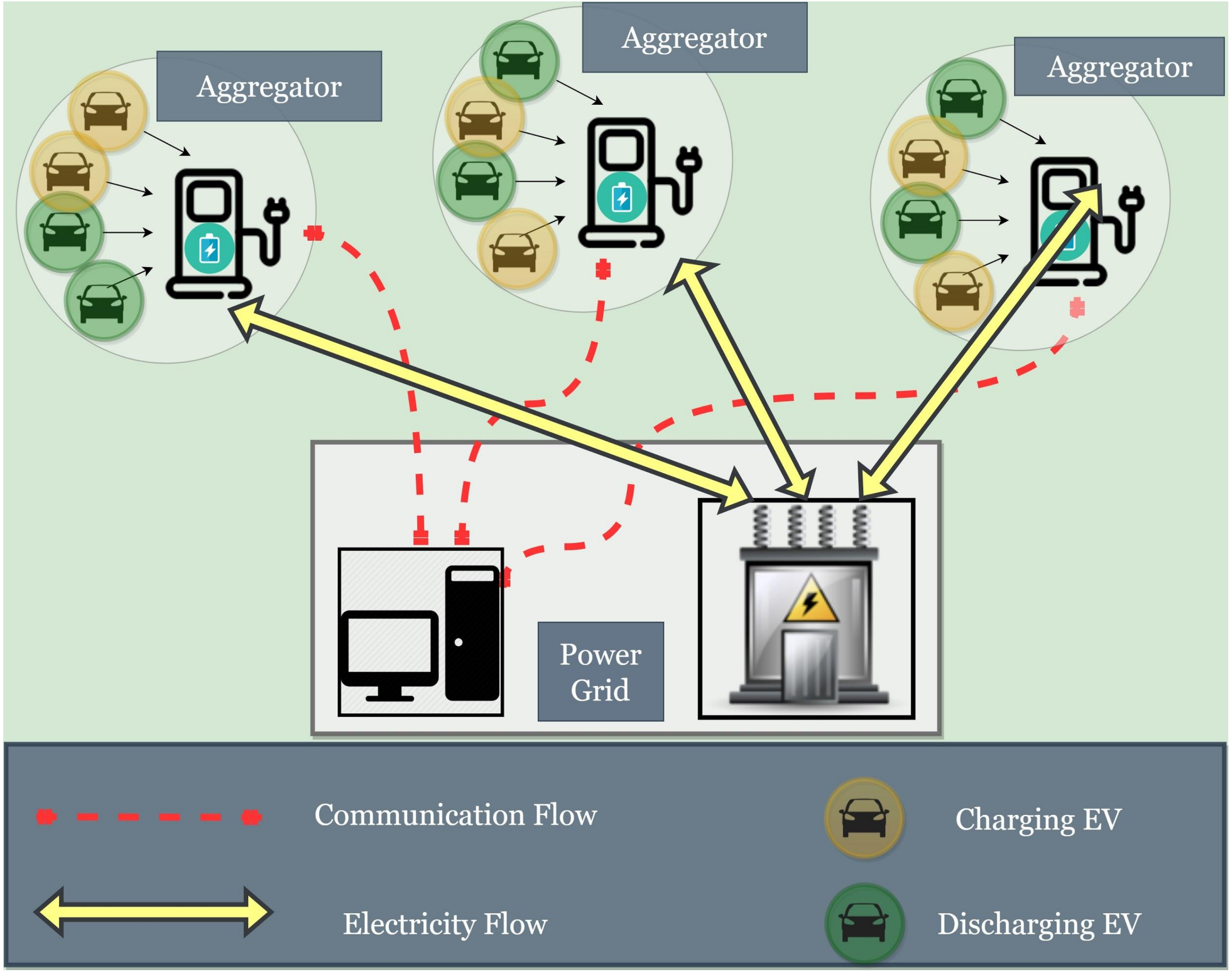
Authors: Gaurang Bansal, Naren, Vinay Chamola

Department of Electrical and Electronics Engineering, BITS Pilani, Pilani Campus, India

Problem

- Ensuring privacy and security in V2G communications
- EV charging stations/ EVs cannot be under 24x7 human supervision
- Device tampering attacks on EVs/ Charging Stations
- Ensure lightweight operation, security and privacy of EV owner.

Network Model



Possible Attacks

- Adversary may tap any communication
- Change, manipulate and withhold data
- Packet Injection
- Store/log messages
- Impersonate EVs or Aggregators
- Try to initiate sessions

Attack Motives

- Gain access to the grid without being noticed.
- Greedy EV owners who want to
  - Recharge their EV's battery for free/ lower prices
  - Cheat service providers to pay more for their EV's power.
- Rouge/unauthorized aggregators who want to
  - Charge EV owners with high prices
  - Take EV's power but not pay the EV owner
  - Gather EV owner info and sell to third parties.
- Criminals who want to
  - Track location/behaviour of EV owners
  - Authenticate with the grid server with someone else's credentials to escape payment

Security Goals

1. Confidentiality
2. Message Integrity
3. Identity Privacy
4. Authentication

Solution

Physical Unclonable Function (PUF) Based Mutual Authentication

Physical unclonable Function (PUF)

- ***A physical unclonable function (sometimes also called physically unclonable function), or PUF, is a physically-defined "digital fingerprint" that serves as a unique identifier for a semiconductor device such as a microprocessor*** - Wiki

- Similar to and as unique as the biometrics of a human.
- Uniqueness comes from physical microstructure variations during fabrication.
- Every single EV can have its own unique “fingerprint”.
- Cannot be cloned or reproduced.

PUF Behavior

Mathematical Function with input C and output K

C: Challenge, K: Response

$$K = PUF(C)$$

PUF Properties

1. If an input C is given to the same PUF many times, it produces the same response K.
2. If the same input C is given to different PUFs, the responses obtained from each PUF differ greatly from each other.

Assumptions

1. PUF is a small hardware component that is present with each participating device and is unique.
2. The communication between a device and its PUF issecure and tamper-proof.

RAMA

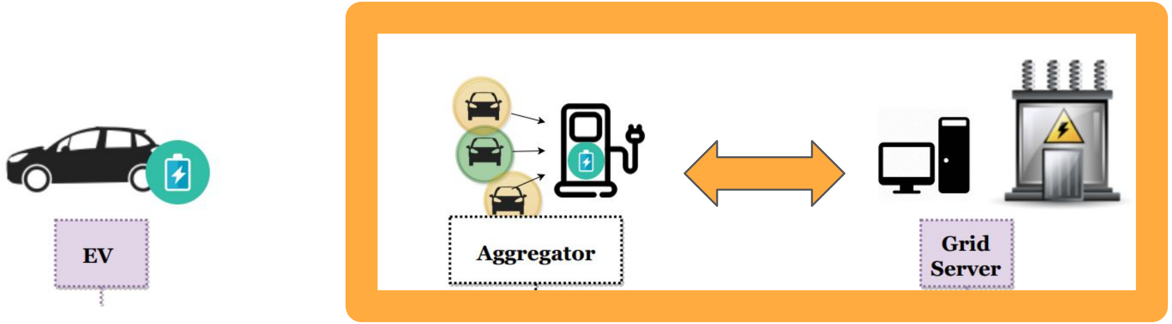
Real-time Automotive Mutual Authentication Protocol Using PUF

New EV deployment

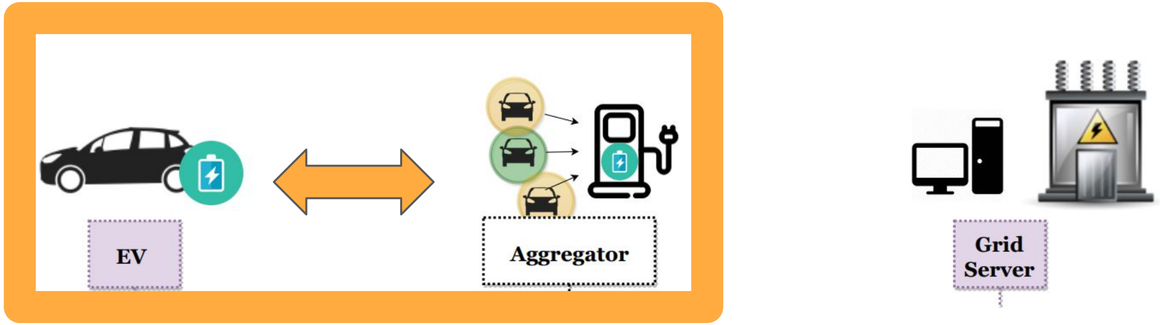
- Server has one (C,K) pair for each vehicle and aggregator.
- Register new EV for V2G services
- (C,K) Acquired through a secure channel established by timed one-time password algorithm (TOTP) by an authorized operator.
- No further operator/TOTP exchange required.

2 Stage Protocol

Aggregator and grid.



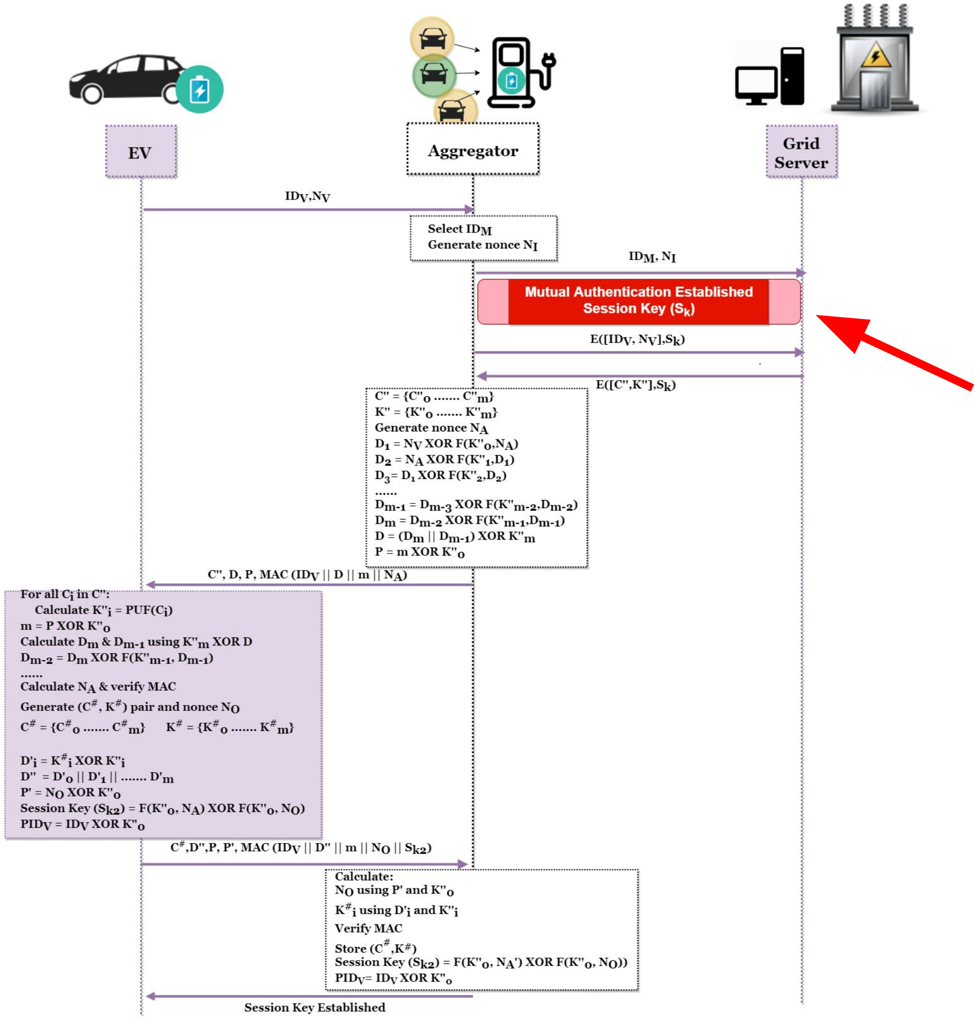
Vehicle and aggregator.



Notations

TABLE I: Notations

Notation	Description
V, ID_V	Vehicle and its ID
M, ID_M	Aggregator(mediator) and its ID
G	Grid Server
$\|$	Concatenation operator
$\oplus$	XOR operation
F	A public non-linear function
$\{Msg\}_k$	Message Msg is encrypted using key k
Msg_{P2Q}	Message Msg is sent from V2G entity P to Q
$MAC(X)$	Message authentication code (MAC) of X
N_A, N_B, N_C N_I, N_O, N_V	Nonces generated at different stages
$(C, K), (C', K')$ $(C'', K''), (C^{\#}, K^{\#})$	Challenge-response pairs of PUF



EV
Aggregator
Grid Server
ID_V, N_V
Select ID_M
Generate nonce N_I
ID_M, N_I
Mutual Authentication Established
Session Key (S_k)
E([ID_V, N_V],S_k)
E([C",K"],S_k)
C" = {C"$_0$ .... C"$_m$}
K" = {K"$_0$ .... K"$_m$}
Generate nonce N_A
D_1 = N_V XOR F(K"$_0$,N_A)
D_2 = N_A XOR F(K"$_1$,D_1)
D_3= D_1 XOR F(K"$_2$,D_2)
......
D_{m-1} = D_{m-3} XOR F(K"$_{m-2}$,D_{m-2})
D_m = D_{m-2} XOR F(K"$_{m-1}$,D_{m-1})
D = (D_m || D_{m-1}) XOR K"$_m$
P = m XOR K"$_0$
C", D, P, MAC (ID_V || D || m || N_A)
For all C_i in C":
Calculate K"$_i$ = PUF(C_i)
m = P XOR K"$_0$
Calculate D_m & D_{m-1} using K"$_m$ XOR D
D_{m-2} = D_m XOR F(K"$_{m-1}$, D_{m-1})
......
Calculate N_A & verify MAC
Generate ($C^\#$, $K^\#$) pair and nonce N_O
$C^\#$ = {$C^\#_0$ .... $C^\#_m$}
$K^\#$ = {$K^\#_0$ .... $K^\#_m$}
D'$_i$ = $K^\#_i$ XOR K"$_i$
D" = D'$_0$ || D'$_1$ || .... D'$_m$
P' = N_O XOR K"$_0$
Session Key (S_{k2}) = F(K"$_0$, N_A) XOR F(K"$_0$, N_O)
PID_V = ID_V XOR K"$_0$
$C^\#$,D",P, P', MAC (ID_V || D" || m || N_O || S_{k2})
Calculate:
N_O using P' and K"$_0$
$K^\#_i$ using D'$_i$ and K"$_i$
Verify MAC
Store ($C^\#$,$K^\#$)
Session Key (S_{k2}) = F(K"$_0$, N_A') XOR F(K"$_0$, N_O))
PID_V= ID_V XOR K"$_0$
Session Key Established

Key takeaways from protocol

1. Nonces to guarantee freshness
2. Lightweight block based encryption mechanism
3. Message Authentication Code (MAC) to verify data integrity, EV/aggregator identity and nonce freshness
4. New (C,K) pair communicated for future authentication (each pair used only once)
5. PUF dependent session keys in both stages
6. Pseudo-ID generated for EV and updated in grid server

Comparison with state-of-the-art schemes

TABLE II: Comparison of Security Features

Features	[22]	[9]	[10]	[12]	[14]	[30]	[24]	RAMA
Mutual Authentication	✓	✓	✓	✓	✓	✗	✓	✓
Identity Protection	✓	✓	✓	✓	✗	✓	✓	✓
Message Integrity	✓	✓	✗	✗	✓	✓	✓	✓
Man-In-The-Middle Attack	✓	✓	✗	✓	✓	✓	✓	✓
Impersonation Attack	✓	✗	✗	✗	✓	✓	✓	✓
Replay Attack	✓	✓	✗	✗	✓	✓	✓	✓
Session Key Security	✓	✓	✗	✓	✗	✓	✓	✓
Physical Security	✗	✗	✗	✗	✗	✗	✗	✓

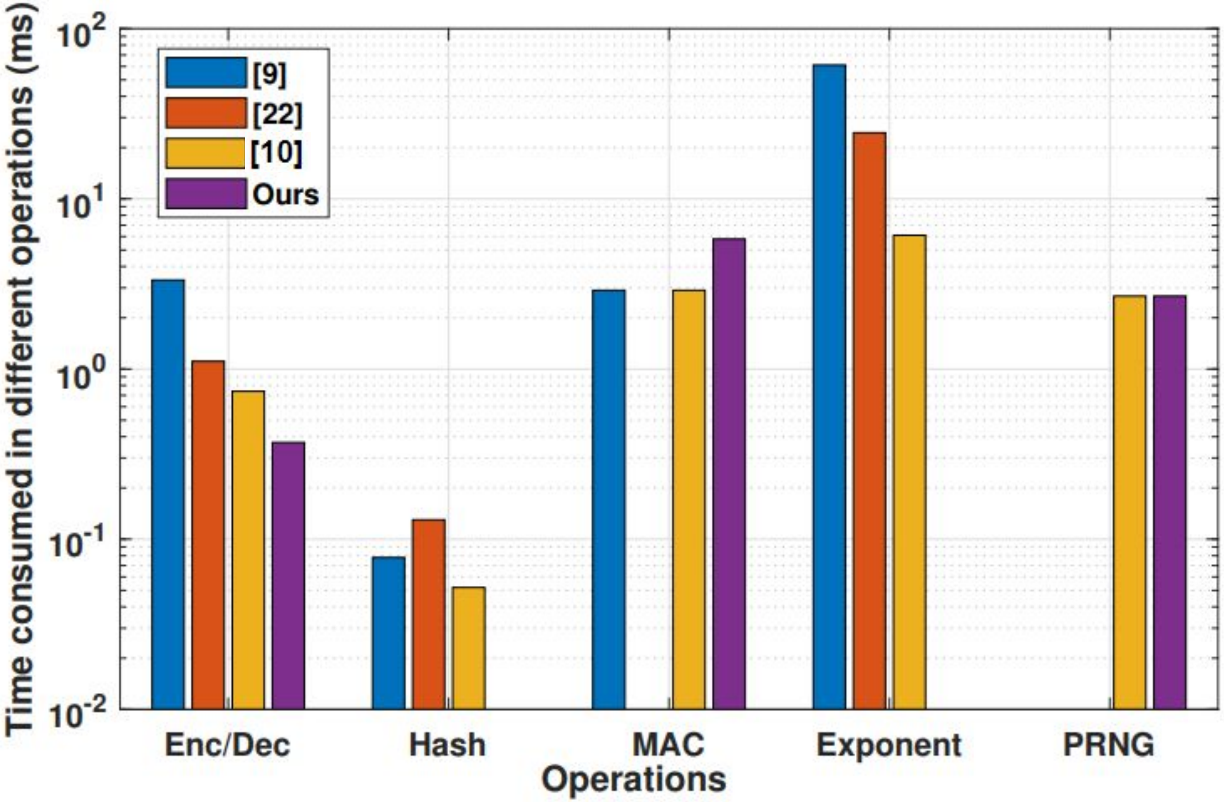
Performance Comparison

[9]: *64.2 ms*

[22]: *25.4 ms*

[10]: *33.1 ms*

Ours: *6.3 ms*



Conclusion

- V2G security provisioning using PUFs
- No secret information stored in EVs/ aggregators.
- One (C,K) stored for every EV and aggregator in grid server.
- Two stage protocol which generates two different session keys.
- Identity protection, message integrity, physical security, and session key security
- Protection against various attacks such as MITM attacks, replay attacks and impersonation attacks.
- simple computations, which makes it very efficient and fast.
- Well suited for V2G applications

Thank you