A Novel User Key Exchange Authentication (NUKA) Scheme for V2G based Frameworks

MCS

By

Aiman Sultan

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security

September 2021

Supervisor Certificate

Certified that final copy of MS / MPhil thesis written by Ms. **Aiman Sultan** student of **MSIS-17** Course Reg.No. **00000277045**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes / Regulations, is free of plagiarism, errors, and mistakes and is accepted as partial, fulfillment for the award of MS / MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: ____________________

Name of Supervisor: **Brig Imran Rashid, PhD**

Dated: ____________________

Signature (HoD): ____________________

Dated: ____________________

Signature (Dean): ____________________

Dated: ____________________

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Aiman Sultan
September 2021

Dedication

This thesis is dedicated to my Family, Teachers, and Friends

for their unconditional love, endless support, and continuous encouragement.

Acknowledgement

All worship and glory be to the All Magnificent and All Merciful Allah Almighty. I am highly obliged and thankful to Almighty Allah for giving me capability and firmness to pursue and accomplish this research and paving way for me despite all the complications and obstacles which have tried to dismount my courage. I am thankful to all my family and particularly my parents for they have always been my pillar of utmost strength and assistance. All this is an outcome of their love and prayers. I owe this degree of mine to my son Muhammad Lazaal Ahmed for being the ultimate source of motivation for me to pursue bigger and better opportunities offered by life.

I pay humble gratitude to my Project Supervisor Brig Imran Rashid, PhD. who not only supervised my research but for mentoring me in a very polite yet considerate and helpful manner. As a supervisor his facilitation and counselling has always been an irreplaceable resource of guidance for me and will continue to be so in coming years of my life. I am also grateful to my worthy committee members Col. Syed Amir Ahsan Gilani, PhD, and Assoc. Prof. Dr. Faisal Amjad as well as Dr. Fawad Khan for their highly helpful comments and suggestion which helped me refurbish my skills and bring a refined edge to this research.

I am deeply grateful to my colleagues being no less than family; PhD scholar Khwaja Mansoor and PhD scholar Mehmood ul Hassan who have guided me wholeheartedly, helped me overcome my limitations and shortcomings and motivating me whenever this objective seemed not achievable. Their sincere advice and trust has brought forth my abilities in a more polished manner. From the beginning of my journey till the last, they have been an embodiment of kindness, motivation and inspiration towards me.

I would like to thank my brother Ahmed Raheeq for his insipirational talks and constant push to help me complete my degree. I can not show my gratitude enough towards my younger sisters Saman & Yusraa, despite their extremely tough medical study and hectic routine of their own, for bearing with me and babysitting my son in my hard times. Their constant support has been a source of full satisfaction for me during my work. I have always resorted to them during my sufferings and have received finest piece of suggestions for decisions regarding my studies as well as life.

Lastly, I express my heartiest thanks and warm wishes to my friends and people around me who have always understood my hectic schedule. Their genuine concern towards my studies is exemplary and their profound contribution can not be put in words and is deeply heartfelt. I appreciate their efforts from the bottom of my heart.

Abstract

Traditional fuel based automobiles are being replaced swiftly with other source oriented vehicles such as solar and electric powered etc. Electric automobiles (EAMs) are one of the emerging and accessible technologies in the transportation sector to decrease CO_2 eruptions and oil demand making up the basis of vehicle to grid (V2G) networks. The V2G systems provide electric energy to Electric automobiles (EAMs) to charge their batteries through aggregating charge stations (ACSs) upon which EAMs are able to function and run. While EAMs are fast replacing conventional Internal Combustion Engines (ICEs), there are emerging threats in terms of security and efficiency in this domain. Since the sensors and devices in V2G frameworks are often resource constraint as no complex hardware is deployed. Mutual authentication among different entities involved in V2G systems, confidentiality and privacy preservation of personal data remains a challenging task. This research proposes a novel user key exchange authentication scheme (NUKA) for V2G based frameworks addressing above mentioned challenges. Informal and formal analysis of NUKA in terms of efficiency and security shows that the proposed scheme is lightweight with enhanced performance and maximum security features as compared to existing schemes.

Contents

List of Figures

List of Tables

List of Abbreviations and Symbols

Abbreviations

EV	Electric Vehicle
V2G	Vehicle 2 Grid
PM	particulate matter
ICE	Internal Combustion Engine
PUF	Physically Unclonable Function
EB	electric battery
BAN logic	Burrows–Abadi–Needham logic
IC	integrated circuit
ROPUF	Ring Oscillator Physically Unclonable Function
MA	mutual authentication

BER	bit error rate
SRAM PUF	Static random access memory PUF
SoCs	system on chips
XOR	exclusive OR
AES	Advanced Encryption Standard
PT	plaintext
CK	ciphertext
MITM	man in the middle
SK	session key
DOS	denial of service
ID	identity
AP3A	Aggregated-Proofs Based Privacy-Preserving Authentication
P^2 **scheme**	Privacy-preserving scheme
BV	battery vehicle
CK model	Canett Krawczyk model
ECC	Elliptic-curve cryptography
MAC	message authentication code
HMAC	Hash-based message authentication code

GS	grid station
EAM	electric automobile
ACS	aggregating charge station
SA	security attribute
PS	proposed scheme

Symbols

IP	input
IP_i	*ith* input
OP	output
OP_i	*ith* output
R_i	*ith* response
F_i	*ith* input feed
PUF_i	*ith* PUF
%	percentage
V	voltage
h_1, h_2, h_3	hash digests
b_1, b_2, b_3	bit strings

$\oplus$	XOR
$\|\|$	concatenation
k	symmetric key
E_k	encryption with key k
D_k	decryption with key k
EAM_i	*ith* EAM
ACS_i	*ith* ACS
M_1, M_2	different messages
ID_{EAM_i}	Id of EAM_i
ID_{GS}	id of GS
K_{ES}	shared key between EAM_i and GS
PID_{EAM_i}	pseudo-identity of EAM_i
K_{GS}	secret key of GS
ID_{ACS_i}	Id of ACS_i
K_{AG}	shared key between ACS_i and GS
SID_{ACS_i}	pseudo-identity of ACS_i
R_S, R_A, n_{eam}	different nonces
$n_c, R_{s_{new}}$	different nonces

N_{EAM_i}	PUF output of EAM_i
N_C	PUF output of ACS_i
T_1, T_2, T_3, T_4, T_5	timestamps
A_1, A_2, A_3, A_4	different verification parameters
$PID_{EAM_{(new)}}$	new pseudo-identity of EAM_i
$h()$	hash operation

Chapter 1

Introduction

1.1 Overview

The exponential increase in technical advancements and inventions in different scientific domains have paved way for enhanced features in automobile industry as well. Traditional fuel based automobiles are being replaced with other source oriented vehicles such as solar and electric powered etc. There are also hybrid vehicles in demand which make use of both conventional fuel i.e. petroleum, diesel as well as battery operated engines [1]. Electric vehicles (EV) are being termed as future of automobile industry as they are easy to manage, require less maintenance, are more environment friendly due to lack of any exhaustive gases and prove much more economical than the traditional cars in the long run. Since electric vehicles require electric power to charge up their batteries and run their engines, they are run in concomitance with the power grid system. This is the basic framework of vehicle-to-grid (V2G) systems [2, 3]. A generic system model of V2G network [3] is shown in 1.1.

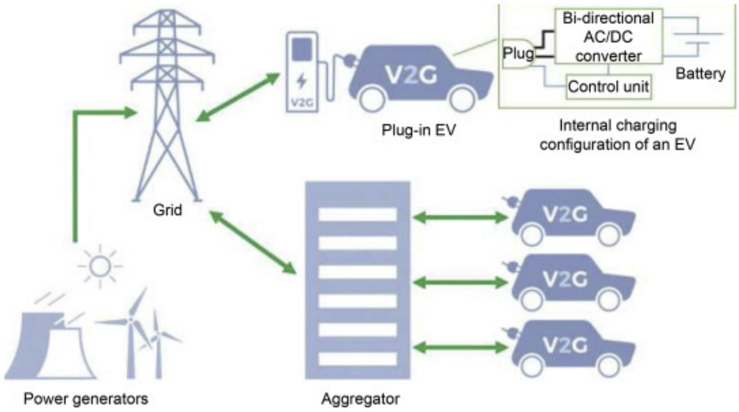


Figure 1.1: Basic V2G Network System

V2G networks are enabled by the batteries in EVs. V2G's goal is to handle energy trading for both battery-powered electric cars and the power grid. This is essential in order to make better use of the grid's electricity. The electrical energy stored in EV batteries may be used to power the grid and other low-energy vehicles. The electrical energy stored in EV batteries may be used to power the grid and other low-energy vehicles. When the grid's load is high, the energy stored in the batteries of electric vehicles (EVs) might be utilised to pump electricity into the grid. When the grid demand is low, on the other hand, the surplus electric power in the grid might be used to charge the EV batteries, reducing waste and minimizing power emissions [2].

The grid systems provide electric energy to Electric Vehicles (EVs) to charge their batteries upon which EVs are able to function and run. Figure 1.2 shows an electric vehicle in a charging state. Generally, a charging station is built and assigned the function to charge the batteries of EVs. These charging stations act as mediating entities between EVs and grid stations and are often termed as aggregators.

Figure 1.2: Electric Vehicle Charging

Communication in these cases is twofold i.e. between EVs and aggregator and between aggregator and grid station. A lot of private and personal data is exchanged during this ‘power charging’ process rising serious threats for security in V2G systems [4]. Also, the sensors and devices employed in V2G frameworks are small, simple, and in-expensive with limited features. They are often resource constraint as no complex hardware is deployed. This poses another threat to security and privacy as an adversary can easily tamper or in some cases, physically capture these devices [5].

Another main issue with simple devices is that security features are often overlooked against efficiency of systems [6, 7]. However, recent researches have shown that security should be regarded as an important and major feature while designing these systems and many different schemes have been put forward addressing these concerns.

1.2 Motivation

Energy self-sufficiency is a key political and social problem for many developing nations, like Pakistan, where over 70% of imported petroleum is used for transportation. This heavy reliance on fossil fuels has resulted in a slew of unwelcome environmental consequences, with two Pakistani cities ranking among the world's top ten polluting cities [8]. The enormous quantity of Carbon dioxide gas (CO_2) emitted by internal combustion engines in automobiles and motorcycles is a major contributor to the problem. Other harmful chemicals like as Sulphur dioxide (SO_2), Nitrogen dioxide (NO_2), and particulate matter (PM), PM10, and PM2.5, will also rise in the atmosphere as a result of increased fossil fuel combustion.

As a result, it is necessary to minimize reliance on fossil fuels and develop more environmentally friendly modes of transportation. Due to the consequences of climate change, Pakistan has already been designated as the sixth most susceptible country. Pakistan has lately opted to move from Internal Combustion Engines (ICEs) to EVs, despite a number of cross-sectoral and multifarious hurdles, with a diversity of policy alternatives for car makers, customers, and global stakeholders. While Pakistan's shift to electric vehicles presents some exciting milestones, a proactive and effective plan is required to track the good elements of rapid advancement and maximize its advantages.

Electric vehicles (EVs) are one of the developing and affordable transportation technologies that can help reduce CO_2 emissions and oil consumption. Other benefits of this approach include minimal noise pollution, cheap maintenance costs, improved safety, energy security, and the possibility to cut peak prices and boost grid stability via vehicle to grid (V2G) power flow. EVs are also prove to be beneficial for Pakistan as it will reduce fuel consumption, will be cost effective and will provide transportation as well energy sources in critical times and far-off geographical terrains where conventional fuels are not available or difficult to make arrangements.

1.3 Advantages and Applications

Major benefits of EVs include lower costs, eco-friendly features and lack of consumption of fossil fuel and thus reduced carbon footprint, reduced pollution, low maintenance needs in the long run, greater convenience, better efficiency and high quality performance. EVs are playing a major role in combating climate change all over the planet. They require lower service costs and shift from conventional transportation to electrical vehicles will show a significant drop in import of oil.

Advanatages of EVs and V2G networks include but are not limited to:

- Public transportation i.e. buses / trains as Electric vehicles are more economical as well as environment friendly in the long run.
- Grid stations providing charging services to not only EVs but also energy storage services.
- Batteries are installed in commercial aircraft to power their electrical equipment. Thermal runway is a well-known issue that causes conventional bat-

teries, particularly lithium-ion batteries, to overheat and catch fire.

- V2G networks might potentially be utilised for power management [9] and storing energy supplied by renewable sources like wind [10]. As a result, V2G for smart grids currently has a variety of practical uses.

1.4 Problem Statement

To address global warming issues, damage caused to ozone layer by combustion gases and pollution through fuel consumption, there is a growing interest in energy self-sufficiency through efficient practices. Energy self-sufficiency is a key political and social problem for many emerging nations, including Pakistan, where transportation accounts for over 70% of imported fuel. Almost the entire transportation industry is reliant on oil-based products, and the Pakistan government spends almost USD 13 billion annually on oil imports [11].

While EVs are fast replacing conventional Internal Combustion Engines (ICEs), there are emerging threats in terms of security and efficiency in this domain. Mutual authentication among different entities involved in V2G systems, confidentiality and privacy preservation of personal data remains a challenging task. A lot of private information is shared between EV and grid station where the need of security and privacy is a major concern. While a lot of research is being carried out in this field, there still remains a lot of threats that are not being tackled in the existing research. The focus of this thesis is to address the need for a protocol that is efficient and secure against all known security threats.

1.5 Research Objectives

The main objectives of thesis are as follows:

- Comprehensive study, comparison and survey of existing authentication schemes for V2G systems
- Proposal of a novel user key exchange authentication scheme for V2G based frameworks
- Formal analysis of proposed scheme in terms of performance, security and efficiency

1.6 Research Methodology

This thesis presents a detailed analysis of Vehicle to Grid (V2G) environments and the numerous security threats that are being faced by this domain. A novel user key authentication scheme is proposed which is based on Physically Unclonable Functions (PUF) to safeguard against threats as well as to provide privacy of electric automobiles' personal information. Existing authentication protocols exhibits security limitations (as reviewed in Chapter **??**). An adversary can launch multiple active and passive attacks on the V2G network to sniff communication, trace credentials and exploit the retrieved data for its own malicious intent. To deal with these vulnerabilities and security risks, a mutual authentication scheme is presented to ensure security against all risks as well as preserving of automobiles' identity. The scheme is lightweight with enhanced performance and maximum security features as compared to existing schemes.

1.7 Thesis Organization

This thesis puts forward a novel user key exchange authentication scheme for V2G based Frameworks. The thesis is documented in the following chapters:

- **Chapter 1:** This chapter presents an overview of V2G networks, motivation for this research, discusses some application areas, puts forward the problem statement, explains the research aims, methodology, and lastly, summarizes the research's contributions.
- **Chapter 2:** This chapter presents some preliminaries. It gives a brief introduction to PUFs and describes the basic cryptographic preliminaries. Threats to V2G networks are presented. It also discusses existing schemes for V2G systems, merits and demerits of existing scheme is explained in detail as well as comprehensive analysis of their security and performance features is presented.
- **Chapter 3:** This chapter discusses the V2G network model and threat model. It also defines the security goals as well as security assumptions for the proposed scheme. It also put forwards a novel user key exchange authentication scheme for V2G based frameworks.
- **Chapter 4:** This chapter presents the formal security analysis of the proposed authentication scheme carried out by Proverif as well as BAN Logic.

It also describes the informal security analysis of the proposed scheme.

- **Chapter 5:** This chapter discusses the performance analysis of proposed scheme in terms of computation, performance and execution time. It presents a comparison analysis of different security features with existing state-of-the-art V2G protocols.

- **Chapter 6:** This chapter presents the results of the thesis study and the shortcomings that were noticed during the process. It also discusses the future aspects of the research.

Chapter 2

Literature Review

2.1 Overview

In this chapter, we will describe some basic preliminaries as well as cryptographic functions. Different challenges that are being faced in a V2G network domain are discussed. Different existing schemes and protocols, their merits and demerits are explained in detail as well as comprehensive analysis of their security and performance features is presented.

2.2 Preliminaries

2.2.1 PUF

PUFs are emerging as a potential approach for defense against cyber-physical attacks. A PUF is a physical characteristic of an integrated circuit (IC) that is unique and unclonable [12]. It's been dubbed the digital fingerprint in recent years; it's as distinctive as human fingerprints [13]. The main feature of PUFs is their lack of requirement for secret keys to be stored in the devices' memory and their reliance on challenge-response pairing between the entities involved such that a challenge yields a specific and discrete response. Another major merit of PUFs is the induction of physical randomness along the process of fabrication variations which ensures that no two same copies can be generated of a single device [14, 15].

A ring oscillator PUF (ROPUF) [16] is shown in figure 2.1.

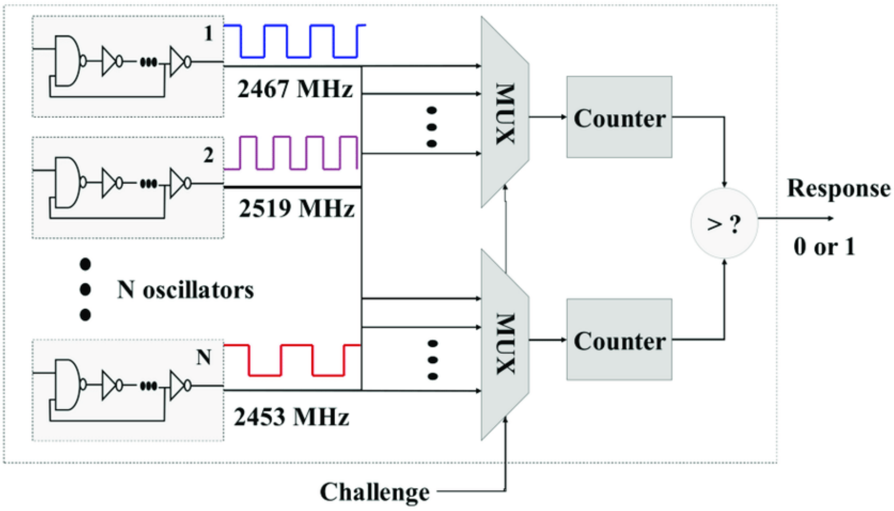


Figure 2.1: Ring Oscillator PUF

A typical ROPUF is constructed by the following components:

- N x frequency oscillators
- 2 x frequency counters
- 1 x comparator
- 2 x two-to-one multiplexers

During a preset time interval, each of the two counters commences counting the number of received cycles from the selected oscillators by the multiplexers. A comparison is carried out by the comparator of the frequency counters' values. A random bit *i.e.* either 1 or 0 is generated as a result of the above comparison process. Since the IC is designed to be arbirtrary and intractable in nature, the results contain a vast spectrum of randomness and unpredictability. A PUF can thus, be generally regarded as one way mathematical function where the challenge or input is mapped to a distinctive response or output. This mapping is mostly based on the circuit's complicated physical structure. Both the challenge or input I and response or output O is in the form of bit strings such that:

$$O = PUF(I) \tag{2.2.1}$$

Assuming a generic PUF with input feed F and output result R, it exhibits the following attributes:

- Diffuseness: Feeding different inputs $F_1, F_2, F_3....F_i$ to one PUF will yield different outputs $R_1, R_2, R_3....R_i$ with high hamming distance.

$$R_i = PUF(F_i)$$

- Uniqueness: Feeding same inputs F to multiple PUFs *i.e.* $PUF_1, PUF_2, PUF_3...PUF_i$ will yield different responses $R_1, R_2, R_3....R_i$ such that $R_1 \neq R_2 \neq R_3 \neq R_i$

high hamming distance.

$$R_1 = PUF_1(F)$$
$$R_2 = PUF_2(F)$$
$$\vdots$$
$$R_i = PUF_i(F)$$

- Reliability: Feeding same input $F_1, F_2, F_3....F_i$ where value of of $F_1 = F_2 = F_3$ and i denotes time instant to one PUF at multiple time instances will yield same responses $R_1, R_2, R_3....R_i$ such that $R_1 = R_2 = R_3 = R_i$ and i denotes the time instant corresponding to input feed. The probability of such feed to output ratio result in the case of ideal scenario with an ideal PUF will be 100%.

$$R_1 = PUF(F_1)$$
$$R_2 = PUF(F_2)$$
$$\vdots$$
$$R_i = PUF(F_i)$$

Since there are always some inconsistencies in various PUF evaluations, the validity of PUF is often less than 100%. Although error-correcting methods like as fuzzy extractors may be employed to address this issue, they would add additional complexity to the MA process [16–18]. As a result, the PUFs used in the proposed protocol must be optimal in nature, *i.e.* devoid of bit errors ensuring 100% availability of V2G system. However, several varieties of perfect PUFs have been designed in recent years that guarantee a 0% Bit-Error-Rate (BER) throughout a wide range of voltage variations as well as temperature [19–21]. A zero percentage of BER in SRAM PUFs is claimed in [22] whereas Jeon *et al.* [23] presented a VIA-PUF design of 0% BER.

The feature that renders PUFs befitting for V2G frameworks is that the ICs are very minute in measurement (*e.g.* few millimeters on scale) and run on low voltage range of 1-5V. It helps achieve a lightweight and efficient scheme to generate security parameters without the need to deploy software or hardware error correction modules. Nonetheless, ideal PUFs are being utilized only for research purposes and are not embedded per se on any System-on-Chip designs (SoCs) and / or on-board computers for V2G entities such as EVs or aggreagting charging stations. This discussion is contemplated as future study and goes over the span of this thesis.

2.2.2 Cryptographic Preliminaries

Some of the cryptographic preliminaries are discussed below:

2.2.2.1 Hash Function

The hash function is defined as a one way function that takes any arbitrary bit string (any length) and outputs a specified length of bit string as a result termed generally as *"hash value"* or *"hash digest"* or more simply as mere *"hashes"* [24]. A generic hash function is shown as below:

bit string of arbitrary length $\longrightarrow$ Hash Function $\longrightarrow$ *hash of specified length*

A hash function exhibits the following properties:

- Given one known hash digest h_1; it is close to impossible to find the input value b_1 that corresponds to that hash digest.
- For any two different bit strings b_1 and b_2, it is very unlikely to find corresponding digests h_1 and h_2 such that $h_1 = h_2$.
- For any two given hash digests h_1 and h_2 such that $h_1 = h_2$ generated by two different bit strings b_1 and b_2, provided b_1 is known, the likelihood to obtain b_2 is extremely low.
- Two bit strings b_1 and b_2 having a switch of just one bit will correspond to digests h_1 and h_2 with more than 50% hamming distance.

These properties of a hash functions make it a predominant primitive in many cryptographic algorithms. Since they are one way, can not be reversed and lightweight in computational operations, that gives the scheme in which they are employed an added security factor as well as enhanced efficiency.

2.2.2.2 Exclusive OR Function

The exclusive OR (XOR) function is widely used in cryptographic algorithms. It responds with a "false: *i.e* 0 when all inputs are similar or evenly distributed and with a "true" *i.e.* 1 if the inputs are oddly distributed. A truth table of XOR with two inputs is given in table 2.1.

Table 2.1: Truth Table of XOR

A	**B**	**O/P**
0	0	0
0	1	1
1	0	1
1	1	0

The operation of XOR is easily reversible if the output and one of the inputs is known. Simply performing XOR with the output with yield the missing input provided there are only two inputs. This is shown below:

$$OP = IP_1 \oplus IP_2$$

$$IP_1 = OP \oplus IP_2$$

$$IP_2 = IP_1 \oplus OP$$

However, it is difficult to deduce multiple inputs from the output of an exclusive OR. This is because XOR is a perfectly balanced operation with equal probability of result being a binary "1" or a binary "0" which makes the deductions in case of long bit strings extremely intensive and increases its effectiveness in cryptographic algorithms.

2.2.2.3 Advanced Encryption Standard (AES)

AES is a block cipher [25] based on iterative structure and Substitution-Permutation Network with specified block length of 128 bits (16 bytes / 4 words). It implies that it processes a data block of 4 columns of 4 bytes (state) taking 128 bits input i.e. plain-text along with key and outputs an encrypted block i.e. cipher-text. Since AES is symmetric key algorithm, same key is used for encryption as well as decryption process. The key size, however, is flexible as it can be 128 bit, 192 bits or 256 bits long.

$$CT = E_k(PT)$$

$$PT = D_k(CT)$$

$$where: PT = plain - text;$$

$$CT = cipher - text;$$

$$E = Encryption\, function$$

$$D = Decryption\, function$$

$$k = symmetric\, key$$

It is extremely difficult to launch attacks on AES and brute forcing an AES algorithm requires $2^{key-length}$ which renders the attempt ineffective and highly extensive. So far, AES is the most secure encryption mechanism being employed all over the research domain [26].

2.3 Major Challenges in V2G Network Domain

This section defines some of the security features required as well as challenges and vulnerabilities currently being faced in design of authentication schemes for a V2G based network.

- **Identity Protection:** In a V2G network, an adversary can obtain identities of different entities *e.g.* aggregator or EVs by identity theft and can misuse these in criminal activity.

- **Forward Secrecy:** A user, after leaving a network, should not have access to any future key elements for any session of that network.

- **Backward Secrecy:** A user, after being authenticated in network should have no access to key information of sessions prior to its entry in that network.

- **Scalability:** One of the biggest challenges in this era of network security is maintenance of security vs efficiency tradeoff. A scheme should be efficient in performance with lightweight primitives while providing adequate security.

- **Eavesdropping / Sniffing Attack:** When an attacker intercepts, deletes, or alters data sent between two entities / users , it is termed as an eavesdropping attack. To access data in transit between entities; eavesdropping, also known as sniffing or snooping, relies on unprotected network interactions.

- **Message Analysis Attack:** Any adversary can capture messages during an ongoing session and analyze the contents passively to launch attack on the network.

- **Impersonation Attack:** An adversary can impersonate a legit entity in a V2G network for its own malicious objectives. It can impersonate an aggregator acting like rogue charge station towards an electric vehicle or vice versa to capture credentials and / or gain access to electrical power.

- **Message Modification Attack:** An adversary can modify a message in a network to change the ongoing session to befit its own illegal intentions. This is a major risk to data integrity in V2G networks.

- **Replay Attack:** When an attacker after eavesdropping on a secure network connection; intercepts it, and then fraudulently delays or resends message or parts of a message to misdirect an entity or server into releasing critical information, this is known as a replay attack.

- **Location Privacy:** In a V2G network, an adversary can obtain location information of different entities *e.g.* aggregator or EVs and can exploit it for any malicious and / or criminal means.

- **Man in the Middle (MITM) Attack:** An attacker after posing as a legitimate user between two authentic entities, not only intercepts but also forwards and in some cases, modify the messages before forwarding them to authentic entity. This attack allows the attacker access to messages and data from both sides.

- **Session Key Security:** A session key is generated and shared between two entities for their secure communication. Its security is a pivotal feature in any protocol as its disclosure will render the whole session insecure and prone to all known security attacks.

- **Physical Security:** Physical security is a key component in a V2G networks as the entities are hardware based *e.g.* EVs, aggregators and grid stations. Physically capturing the devices will lead an adversary to all the information stored on device's memory. This information can contain identity parameters, session keys as well as other verifiers required for registration / authentication etc.

- **Traceability:** All communications in a network between different entities should be carried out in such a way that no outsider can create or track a pattern to be used or exploited to gain behavioral information. This makes it easier for an adversary to impersonate an authentic entity in a network.

- **Denial of Service (DOS) Attack:** A Denial of Service (DoS) attack is basically attempts to cease a network's ongoing sessions and thus rendering it unreachable to its legitimate users. An adversary can try to authenticate itself by flooding the grid station multiple requests through aggregator so much that actually needy Evs can not get through this high traffic to an aggregator to get their electric power service.

- **Cyber Physical Attacks:** An adversary can access control on any entity that has an influence on the physical environment. In a V2G network, a malicious user can take control of an aggregator to alter the electric power voltage as well as switch it on / off at per its own intention causing socioeconomical damage.

2.4 Related Work

The idea of Vehicle to Grid (V2G) systems was first coined by Kempton and Tomić [27] back in 2005. In less than two decades, infrastructure of V2G systems has seen a lot of progress and evolution [28–32]. However, secure communication between entities involved (grid stations, electric automobiles and aggregators etc.), security threats and privacy preservation are some of the major concerns. Tradeoff between security and efficiency is a challenging task in this domain. Many protocols have been put forward to tackle these issues but a scheme is yet to be presented which addresses all the current security issues and is proved to be resistant against all known security threats.

V2G network security and its major challenges were described by Saxena *et al.* in [33]. The article provided a comprehensive analysis of V2G network covering it from all involving entities' perspective i.e. vehicle owner's, vehicle's, vehicle battery's, electric utility's (charging stations / booths), billing company's (involving offline / online banking transactions and corresponding flow of private and personal information). This scheme made use of anonymous signatures, remote attestation and secure payment methods to provide anonymous authentication, non-repudiation, access control and information integrity. The article's formal security proof claimed it to be secure against impersonation attack, man in the middle (MITM) attack, redirection attack, known key attack and replay attack.

This scheme however is prone to cyber-physical attacks, their detection and prevention i.e. tampering or capture of devices in V2G as well as traceability and rogue impersonation attacks.

A novel scheme addressing privacy preserving concerns with respect to electric vehicles' battery is presented in [34]. The scheme P^2 provides mutual authentication and secure transfer of information between individual electric vehicles and an aggregator without leakage of any personal information i.e. vehicle battery's identity and location etc. This is achieved by using cryptographic algorithms of partially blind signatures [35] and ID-based searching protocol. The article also discusses the rewarding schemes and benefits reaped by electric vehicle batteries after their services that are considered pivotal in deployment of V2G frameworks. This scheme provides security features of mutual authentication, data secrecy, privacy preservation and integrity. It is also resistant to MITM attack, known key attack and replay attack. It however lacked a formal security proof and this scheme does not provide any security against impersonation attack and cyber-physical attacks.

Liu *et al.* presented $AP3A$ in [36] which provides capability of keeping track of a vehicle presence or absence in its home network. The article put forwards a scheme where instead of providing individual power status, AP3A transmits the aggregated power status of the cars linked to an aggregator, ensuring privacy for each EV. This ensures the privacy of identity of individual EVs. This scheme is simple employing simple operations of XOR, hash functions and few exponentials. Authors claim that their scheme is resistant towards impersonation attack, replay attack, denial of service (DOS) attack and provides security features of mutual authentication between EVs and aggregators, privacy of identity and secure identification of different nodes in a complex V2G network. The scheme, however, is vulnerable to secure transaction integrity, MITM attack, session key security and cyber-physical attacks.

Another scheme was put forward by Liu *et al.* in [37] switching from identity based protocol to role based protocol to address privacy preservation issues in V2G networks. Their scheme is based on the notion that an electric vehicle's battery can be an energy consumer, storage entity as well as energy generating unit. The article ensures privacy preservation for all above mentioned roles of Battery vehicles (BV) instead of their individual identities. Their scheme makes use of many cryptographic protocols i.e. ring signature, fair blind signature, and proxy re-encryption to provide security features of mutual authentication between EV and aggregator, anonymity, hierarchical access control, session key security, data confidentiality and integrity. It is resistant against traceability attack but is vulnerable to replay attack, impersonation attack and cyber-physical attacks.

A secure key distribution scheme is presented in [38] for smart grids. The authors employed identity based searchable encryption protocol [39] and identity based signature scheme [40] to introduce a novel key distribution mechanism. It introduces anonymity and supports mutual authentication. The article provides a comprehensive formal security proof of the proposed scheme. Authors claim their scheme to provide perfect forward secrecy, enhanced efficiency as well as resistance against unknown key share attack. The major vulnerabilities of this scheme are its susceptibility towards impersonation attack, replay attack, MITM attack and cyber-physical attacks.

The major vulnerabilities in [38] were addressed by Odelu *et. al.* who presented a secure authenticated key agreement scheme [41] under the extensively recognized Canett Krawczyk (CK) adversary model [42] for smart grids. The authors put forward a scheme's formal security proof showing secure mutual authentication between smart meters and service provider(s). The scheme makes use of bilinear pairings, Identity based Encryption and ECC based ElGamal type Digital Signatures. The schemes maintains to be resistant against impersonation attack, reply attack and unknown key share attack. It also claims to provide perfect forward secrecy, session key security and credentials security of strong high meters. The scheme is vulnerable to man in the middle attack, traceability and physical security issues.

Another lightweight secure authentication scheme for V2G systems ensuring privacy preservation is introduced in [43]. The scheme allows EVs to create their own pseudonym identities and, as a result, they do not provide their personal information to anyone in the V2G network i.e. aggregator or grid station. In this way, the EVs' privacy is not threatened during the (dis)charging process. The scheme also introduces a secure authentication mechanism that ensures that no EV can behave maliciously by allowing grid station to monitor and trace EV's behavior, electric transactions during (dis)charging process as well as maintenance of integrity and confidentiality of messages exchanged during electric transactions during (dis)charging process. It is lightweight as the number of messages exchanged between EV(s) and grid station during transactions is less than other existing schemes and thus, makes use of less resources and create less overhead as a result. The scheme is based on BlueJay ultra-lightweight hybrid cryptosystem [44]. The suggested protocol makes use of bilinear pairing as well as decisional Diffie–Hellman assumption are used to produce the key parameters. It also employs a pseudorandom number generator AKARI-2 [45] for generation of pseudo-identities and symmetric keys. To protect the user's privacy, partially blind signature methodology and zero-knowledge proof is used. The proposed scheme provides security features of identity protection of EVs, session key security and message integrity. It is resistant against MITM attack, impersonation attack and replay attack. It does not provide mutual authentication as only EVs are authenticated by grid stations. It is also susceptible to cyber-physical attacks.

For privacy-preserving key agreement mechanism in V2G networks, Shen *et al.* put forward a novel scheme in [46]. It establishes a self-synchronization technique to maintain privacy and the inclusion of a session key in their protocol provides enhanced security. The scheme provides security features of anonymity and perfect forward secrecy and is claimed to be resistant against impersonation attack, replay attack, de-synchronization attack and stolen smart card attack. However, this schemes is found susceptible to man in the middle attack and cyber-physical attacks. The vulnerabilities in the protocol includes lack of location privacy and session key integrity.

Multiple Authentication protocols for V2G environment have been discussed in [47–49]. Saxena *et al.* presented a mutual authentication protocol in [50] which is based on bilinear pairings technique with functionality of batch verification by an accumlator and privacy preservation of EVs. Their scheme claims to be more efficient in terms of low computations and generates lower communication overheads. It provides security features of anonymity of vehicle, forward privacy and message integrity. It is also resistant to MITM, replay and redirection attacks as well as impersonation attack. It is prone to de-synchronization attack and cyber physical attacks.

Gope and Sikdar offer a lightweight mutual authentication mechanism [51] based on one-way noncollision hash algorithms. Another scheme by the same authors was presented [52] that claims to be lightweight and provides privacy preservation, location privacy for V2G environments. It also offers low compuational costs at EVs' node. It lacks physical security features.

Another lightweight scheme for message authentication is proposed by Fouda *et al.* in [53]. Meters at various levels of the smart grid are mutually authenticated, and a shared session key is generated which, in conjunction with a hash-based authentication code technique is used to provide efficient message authentication. Although this method was designed for smart grid communications, it may easily be used to V2G networks as well. Another scheme [54] using hash codes for authentication provides forward / backward secrecy, message integrity and security against collusion attack but is susceptible to replay, masquerade and cyber physical attacks. It also lacks the security features of location privacy and session key integrity.

Tao *et al.* presented a protocol *AccessAuth* [55] considering constraints of all entities in a V2G based network environment. It features a capacity based access control mechanism. It allows mutual authentication and a setup to be built as per the capacity overhead of the network. It also provides functionality of session abrogation as well as recovery along with forward secrecy. The schemes lacks a formal security proof and is susceptible to many security threats *e.g.* cyber physical attacks, MITM and replay attacks.

A novel authentication scheme featuring privacy preservation was proposed by Su *et al.* in [56]. It makes use of nonsupersingular elliptic curve for its communication mechanism. It provides higher security but it uses heavy cryptographic algorithms. It claims to be resistant towards replay attack and provides identity privacy of all EVs. However, their scheme is susceptible to threats concerning location privacy, identity privacy from internal network's entities, rogue charging station, impersonation attacks as well as physical security.

Abbasinezhad-Mood *et al.* presented an escrow-less Chebyshev chaotic map based key agreement protocol [57] for V2G environments. The authors claimed their scheme to be resistant against replay attack and more efficient with better performance in terms of time and computations. It however, lacks the security feature of location privacy, identity privacy from internal network's entities and threats from rogue charging station location. It is also susceptible to impersonation attack, MITM and cyber physical attacks.

Bansal *et al.* in [58] introduced mutual authentication scheme for V2G networks by use of Physical Unclonable Function (PUF) [59]. The scheme provides mutual authentication between EV and grid station by mutually authenticating EV and aggregator as well as aggregator with grid station. Authors discussed a comprehensive formal security proof of their scheme by Mao and Byod Logic [60]. The article claims their scheme provides security features of mutual authentication, session key security, message confidentiality and integrity. The proposed protocol is secure against many security threats including MITM attack, replay attack, impersonation attack and provides physical security as well. The scheme, however, lacks features of location privacy, EV's privacy against aggregators and is less efficient with respect to computational costs at EVs' end. It is susceptible to anonymity threats, traceability issues, DOS attack, rogue aggregator attack, stolen verifier attack, DOS attack and cyber-physical attacks.

A novel PUF based authentication scheme is proposed in [61] for V2G networks. The scheme is lightweight and uses PUF based responses to establish mutual authentication between entities in V2G network. It provides message confidentiality & integrity, user as well as location privacy and physical security. Their scheme's security analysis shows the scheme is resistant against replay attacks, impersonation attacks, data analysis threats and message injection attack. Despite being lightweight and efficient than many existing schemes, it is susceptible to traceability threats, anonymity issues, MITM, session key security attacks and rogue aggregator attacks.

Multiple authentication techniques that operate in the realm of V2G networks are available in the literature. These techniques are generally constraint in terms of their efficiency, either involve a lot of computing, or have multiple security flaws. A comprehensive comparison of discussed schemes along with their characteristics, security features and vulnerabilities is presented in table 2.2.

Table 2.2: Authentication schemes for V2G based Networks

Scheme	**Based on**	**Security Features**	**Susceptibilities**
Saxena *et al.* [33]	anonymous signatures, remote attestation and secure payment methods	anonymous authentication, non-repudiation, access control and information integrity; secure against man in the middle (MITM) attack, redirection attack, known key attack and replay attack	prone to cyber-physical attacks, their detection and prevention i.e. tampering or capture of devices in V2G as well as traceability and rogue impersonation attacks.
P^2 [34]	partially blind signatures and ID-based searching	mutual authentication, data secrecy, privacy preservation and integrity; resistant to MITM attack, known key attack and replay attack	lacked a formal security proof, vulnerable to impersonation attack and cyber-physical attacks

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
AP3A [36]	XOR, hashes and few exponential functions	ensuring privacy for each EV; resistant towards impersonation attack, replay attack, denial of service (DOS) attack, mutual authentication, privacy of identity and secure identification of different nodes in a complex V2G network	vulnerable to secure transaction integrity, MITM attack, session key security and cyber-physical attacks
Secure Key Distribution Scheme [38]	identity based searchable encryption, signatures	supports mutual authentication, provides anonymity, perfect forward secrecy, enhanced efficiency, resistance against unknown key share attack	vulnerable to impersonation attack, replay attack, MITM attack and cyber-physical attacks

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
Liu *et al.* [37]	ring signature, fair blind signature, and proxy re-encryption	privacy preservation of BV, mutual authentication, anonymity, hierarchical access control, session key security, data confidentiality and integrity, resistant against traceability attack	vulnerable to replay attack, impersonation attack and cyber-physical attacks
Odelu *et. al.* [41]	bilinear pairings, Identity based Encryption and ECC based ElGamal type Digital Signatures	perfect forward secrecy, session key security and credentials security of strong high meters; resistant against impersonation attack, replay attack and unknown key share attack	vulnerable to man in the middle attack, traceability and physical security issues

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
Abdullah *et. al.* [43]	BlueJay ultra-lightweight hybrid cryptosystem, bilinear pairing, decisional Diffie–Hellman, AKARI-2, partially blind signature methodology and zero-knowledge proof	allows EVs to create their own pseudonym identities, identity protection of EVs, session key security and message integrity; resistant against MITM attack, impersonation attack and replay attack	no mutual authentication and prone to cyber-physical attacks
Shen *et al.* [46]	self-synchronization technique for privacy preservation	provides anonymity & perfect forward secrecy; resistant against impersonation attack, replay attack, de-synchronization attack and stolen smart card attack	lack of location privacy and session key integrity; susceptible to MITM, cyber-physical attacks

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
Saxena *et al.* [50]	bilinear pairings technique with accumulator based batch verification	efficient with low computations & lower communication overheads; provides anonymity of vehicle, forward privacy, message integrity; resistant to MITM, replay and redirection attacks, impersonation attack	prone to de-synchronization attack and cyber physical attacks
AccessAuth [55]	capacity based access control mechanism	provides mutual authentication as per capacity overhead of NW, functionality of session abrogation & recovery, forward secrecy	lacks a formal security proof; susceptible to cyber physical attacks, MITM and replay attacks.
Gope and Sikdar [52]	one-way noncollision hash algorithms	lightweight; offers privacy preservation, location privacy; low computational costs at EVs' node	lacks physical security features

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
Su *et al.* [56]	nonsupersingular elliptic curve	resistant towards replay attack; provides identity privacy of all EVs	heavyweight design; susceptible to threats concerning location privacy, identity privacy from internal network's entities, rogue charging station, impersonation attacks, physical security
Abbasinezhad Mood *et al.* [57]	escrow-less Chebyshev chaotic map	resistant against replay attack; more efficient with better performance in terms of time and computations	lacks location privacy, identity privacy; susceptible to rogue charging station, impersonation attack, MITM, cyber physical attacks

Continuation of Table 2.2			
Scheme	**Based on**	**Security Features**	**Susceptibilities**
Bansal *et al.* [59]	Physical Unclonable Function (PUF), MAC, hash functions	provides mutual authentication, session key security, message confidentiality & integrity; secure against many security threats including MITM attack, replay attack, impersonation attack; provides physical security	lacks location privacy, EV's privacy against aggregators; high computational costs at EVs' end; susceptible to anonymity threats, traceability issues, DOS attack, rogue aggregator attack, cyber-physical attacks
Kaveh *et al.* [61]	PUF, hash functions	lightweight; provides mutual authentication, message confidentiality & integrity, location privacy, physical security; is resistant against replay attacks, impersonation attacks, data analysis threats, message injection attack	susceptible to traceability threats, anonymity issues, MITM, session key security attacks, rogue aggregator attack
End of Table			

2.5 Summary

This chapter discussed some basics for V2G networks *i.e.* PUF in detail and some cryptographic preliminaries briefly. Threats to V2G networks were presented. It also discussed existing schemes for V2G systems with their merits as well as demerits. Their differences and a comprehensive analysis of their security and performance features is presented in a tabular form. Chapter 3 will present the V2G network model and proposed work.

Chapter 3

Proposed Work

3.1 Overview

In this chapter, we will describe the network model of V2G based frameworks. A detailed description of entities and their communication flow is given for better understanding of V2G network. Security goals and assumptions will be discussed. We will present our proposed mutual authentication protocol with all phases discussed in detail. The research includes the following contributions:

- A novel user key exchange authentication scheme for V2G based frameworks is presented in this chapter. The scheme is based on Physically Unclonable Function (PUF) and provides maximum security against known threats.
- The scheme is analysis for its security features by Proverif and BAN Logic. An informal security analysis is also presented discussing multiple security features and describing scheme's resistance to different security attacks.

- The scheme is lightweight with employing light cryptographic primitives and generate low computational overheads.

The security analysis is carried out in detail in chapter 4 and performance analysis is described in chapter 5 respectively.

3.2 System Model

3.2.1 Network Model

The network model of a vehicle to grid (V2G) domain consists of 3 major entities:

1. **Grid Station**: The grid station GS is the main entity in V2G network that provides electric power to Electric Automobile EAM to charge its battery on some predefined cost by a commercial enterprise. This is carried out through Aggregating Charge Station ACS. The GS has many resources as compared to ACS and EAM and can easily perform high computations at its end. It also has high memory storage and stores credential data *i.e.* identities, pseudo-identities, session keys, security parameters etc. at its server.

2. **Aggregating Charge Station**: The Aggregating Charge Station ACS is intermediary entity between a grid station GS and an Electric Automobile EAM and provides charging as well as discharging services. All the communication (credentials / security parameters) flow from EAM to GS is carried

out through ACS. Although the ACS has lower resources than GS, it still has more memory and computational capabilities than EAM.

3. **Electric Automobile**: The Electric Automobile EAM is the vehicle with installed electric battery (EB) and requires electric power to run. It charges up its EV from GS through the nearest ACS. This battery charging is two-way. In case of high load on grid systems, the power stored on EAM's EB can be utilized to pump power onto GS as well as gaining electric power from GS when EBs fall short of their charging.

Any EAM in need of charging requires to get the electric power supply from the GS. For this purpose, there needs to be some authentication mechanism to be carried out so as to identify the authentic EAM and cross-check it by the data stored on the GS. Since, all the communication between a EAM and GS is carried out through ACS, there is an equally crucial need for authentication of that ACS. It implies that both the EAM and ACS need to be authenticated by the GS. This is carried out with the registration of both these entities before the actual mutual authentication phase so that any EAM or ACS needs not to be registered and thus authenticated again and again at GS. Also, the EAM needs to be authenticated by both ACS and GS. Thus, the GS generates and shares two keys for every session:

- a shared key between GS and ACS
- a shared key between GS and EAM

When any EAM requires electric power to charge up its EB, it goes to the nearest

ACS. Since their identities along with their physical location is already stored on *GS*, a mutual authentication setup is carried out. Both *EAM* and *ACS* have PUFs embedded in their hardware which generates a unique unclonable parameter that plays a crucial part in that mutual authentication setup. After the mechanism is complete, the *EAM* charges up its *EB* through *ACS* and pays up for its services according to the settled charges. In all this mutual authentication scenario, The *EAM* doesn't communicate with *GS*, the *GS* communicates with *ACS* and *ACS* communicates with both *GS* and *EAM*. All this communication is carried out over a non-secure public channel.

The network model of a vehicle to grid (V2G) domain is shown in fig 3.1.

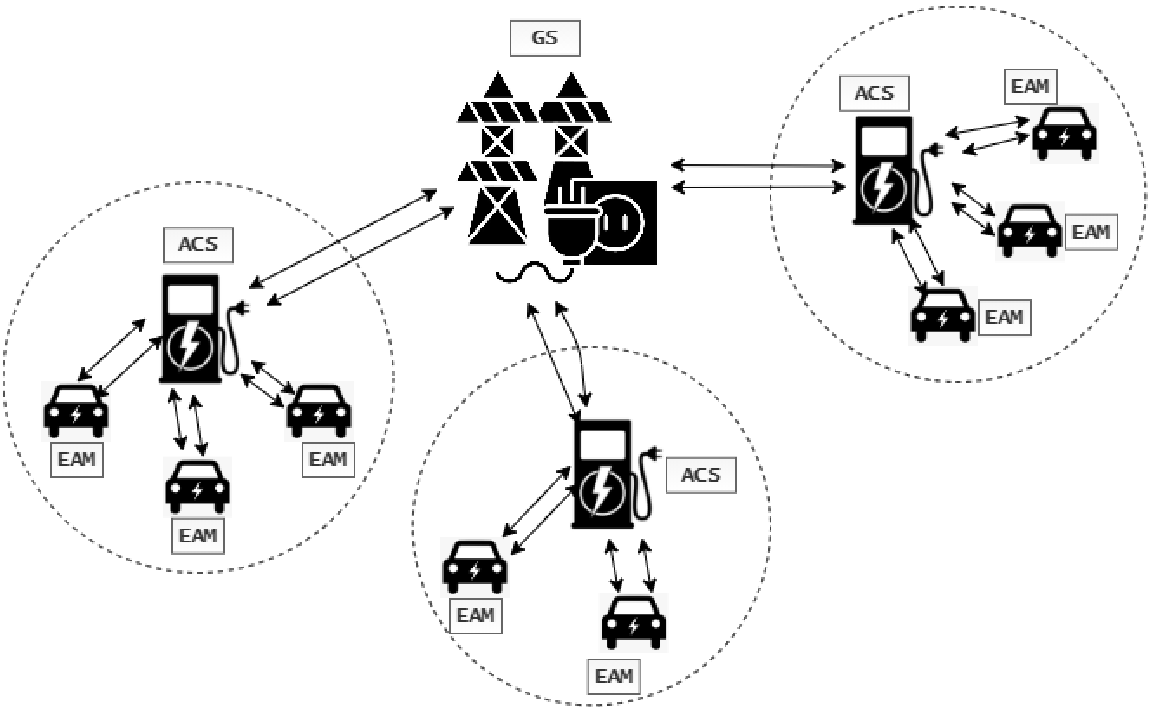


Figure 3.1: V2G Network Model

3.2.2 Threat Model

A threat model is defined where an adversary's main objective is to gain unauthorized access to grid station. Since the communication of V2G network is carried out over a public channel, the data can easily be intercepted by an adversary. The adversary can have the following capabilities:

- Sniffing and capture of data packets
- Administer modification of messages
- Store old captured packets to start a communication at some later time by impersonating an authentic entity
- Intercept and take active part in an ongoing session by launching MITM attack

If an unauthorised or potentially hazardous party is able to authenticate with the GS, electric power transfers to authentic ACS might be effected and / or disrupted and can lead to economic stagnation. Adversary in this threat model can be any of the following with some malicious intent:

- EAM owners trying to take advantage of the V2G technology to receive free charging for their automobiles or to extract more money from the service provider when they provide electric power from their EAM to the GS.
- Rogue or unlicensed / non-registered ACS trying to cause fraudulent activities to extract exorbitant fees from EAM for the electric power service.

- Rogue or unlicensed / non-registered ACS failing intentionally to compensate the EAM owner for the electric power they obtain during the discharging process in case of low load on GS.

- A rogue ACS may also leak / sell the EAM owner's personal credentials without their consent to third-party where this information can be used in illegal activities.

- Delinquents wishing to track behaviour / location of some EAM visits to a specific ACS and making use of that behavioral history to get authenticated by ACS under fake credentials to avoid electric service payments.

3.2.3 Security Goals

Following security goals are defined for this research:

1. **Mutual Authentication:** Before any electric power transaction is initiated, all entities *i.e.* EAM, ACS and GS must be mutually authenticated to ensure security from any kind of impersonation attacks.

2. **Anonymity:** Since the communication is carried out over a public channel, the location and identity of both the electric automobile EAM and aggregating charge station ACS should be masked in such a way that any eavesdropping fails to fetch details about any entity's private credentials.

3. **Communication Secrecy:** The entire communication should be obstructed such that a packet capture yields no useful knowledge of the transaction in-

formation.

4. **Communication Integrity:** All the entities $i.e. EAM, ACS$ and GS should be able to perform verification of any received message from its source. Any message found to be replayed and / or altered should be dropped and session should be terminated there and then to ensure communication integrity.

3.2.4 Security Assumptions

The following assumptions are made in this research:

- The grid station GS is regarded as a trusted entity and all credentials as well as keys stored on grid server are secure.

- All the registrations of multiple electric automobiles EAM_i and aggregating charge stations ACS_i with grid station GS are carried out over a secure channel that can not be intercepted by any unauthorized entity.

- The EAM_i and ACS_i have lower computational capabilities and storage as compared to GS.

- All electric automobiles EAM_i and aggregating charge stations ACS_i have their own unique PUFs implanted in their hardware.

- The parameters generated by a PUF are reliable, can not be vandalized and / or created by any other cryptographic algorithms.

3.3 Proposed Mutual Authentication Protocol: Novel User Kye-Exchange Authentication (NUKA)

The proposed scheme consists of three phases *i.e.*

1. Electric automobile EAM Registration Phase
2. Aggregating charge station ACS Registration Phase
3. Mutual Authentication MA Phase

These phases are described in detail as follows:

3.3.1 Electric Automobile Registration Phase

The whole communication in electric automobile registration phase is executed over a private and secure channel. It is carried out as follows:

- The electric automobile EAM_i generates it's identity ID_{EAM_i} and send it to the GS.

$$M_1 = \{ID_{EAM_i}\} \tag{3.3.1}$$

- The grid station GS generates a nonce R_S, concatenate it with the identity of electric automobile ID_{EAM_i}, calculates its hash value and XOR it with it's own identity *i.e.* ID_{GS} to compute shared key K_{ES} between EAM_i and

GS.

$$K_{ES} = h\left(ID_{EAM_i} || R_S\right) \oplus ID_{GS} \tag{3.3.2}$$

- It then generates a pseudo-identity PID_{EAM_i} of EAM_i by concatenating identity of electric automobile ID_{EAM_i} and nonce R_S and then encrypting it with AES using its own secret key $E_{K_{GS}}$.

$$PID_{EAM_i} = E_{K_{GS}}(ID_{EAM_i} || R_S) \tag{3.3.3}$$

- The parameters $ID_{EAM_i}, K_{ES}, PID_{EAM_i}$ are stored at grid station and it sends a message M_2 to EAM_i containing secret shared key K_{ES} and pseudo-identity of electric automobile PID_{EAM_i}.

$$M_2 = \{K_{ES}, PID_{EAM_i}\} \tag{3.3.4}$$

- The EAM_i stores both these parameters.

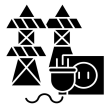
The electric automobile registration phase is shown in table 3.1.

3.3.2 Aggregating Charge Station Registration Phase

The entire communication of this phase is carried out over a private and secure channel. The steps are implemented as follows:

- The aggregating charge station ACS_i generates it's identity ID_{ACS_i} and

Table 3.1: Electric Automobile Registration Phase

		
EAM_i		GS
Generate ID_{EAM_i}		
	$\xrightarrow{M_1=\{ID_{EAM_i}\}}$	
		Generate: nonce R_S Compute: $K_{ES}=h(ID_{EAM_i}\|\|R_S)\oplus ID_{GS}$ Generate: $PID_{EAM_i}=E_{K_{GS}}(ID_{EAM_i}\|\|R_S)$ Store: $\{ID_{EAM_i},K_{ES},PID_{EAM_i}\}$
	$\xleftarrow{M_2=\{K_{ES},PID_{EAM_i}\}}$	
Store: K_{ES},PID_{EAM_i}		

send it to the GS via a secure channel.

$$M_1=\{ID_{ACS_i}\} \tag{3.3.5}$$

- The grid station GS generates a nonce R_A, concatenate it with the identity of aggregating charge station ID_{ACS_i}, calculates its hash value and XOR it with it's own identity *i.e.* ID_{GS} to compute shared key K_{AG} between ACS_i and GS.

$$K_{AG}=h\left(ID_{ACS_i}||R_A\right)\oplus ID_{GS} \tag{3.3.6}$$

- It then generates a pseudo-identity SID_{ACS_i} of ACS_i by concatenating identity of aggregating charge station ID_{ACS_i} and nonce R_A and then encrypting

Table 3.2: Aggregating Charging Station Registration

ACS_i		GS
Generate ID_{ACS_i}		
	$M_1=\{ID_{ACS_i}\}$ $\longrightarrow$	
		Generate: nonce R_A Compute: $K_{AG} = h(ID_{ACS_i}\|\|R_A) \oplus ID_{GS}$ Generate: $SID_{ACS_i} = E_{K_{GS}}(ID_{ACS_i}\|\|R_A)$ Store: $\{ID_{ACS_i}, K_{AG}, SID_{ACS_i}\}$
	$\longleftarrow$ $M_2=\{K_{AG}, SID_{ACS_i}\}$	
Store: K_{AG}, SID_{ACS_i}		

it with AES using its own secret key $E_{K_{GS}}$.

$$SID_{ACS_i} = E_{K_{GS}}(ID_{ACS_i}||R_A) \tag{3.3.7}$$

- The parameters $ID_{ACS_i}, K_{AG}, SID_{ACS_i}$ are stored at grid station and it sends a message M_2 to ACS_i containing secret shared key K_{AG} and pseudo-identity of aggregating charge station SID_{ACS_i}.

$$M_2 = \{K_{AG}, SID_{ACS_i}\} \tag{3.3.8}$$

- The ACS_i stores both these parameters.

The registration phase for aggregating charge station is shown in table 3.2.

3.3.3 Mutual Authentication Phase

The mutual authentication phase between a EAM_i and GS is shown in table 3.3 and is carried out in the following steps:

1. At EAM_i:

   - The electric automobile EAM_i selects its pseudo-identity PID_{EAM_i}.
   - It inputs a nonce n_{eam} to its PUF and generates N_{EAM_i}.

$$N_{EAM_i} = PUF\left(n_{eam}\right) \tag{3.3.9}$$

   - After that, it computes the parameter N_Z by taking XOR of N_{EAM_i} and K_{ES}.

$$N_Z = N_{EAM_i} \oplus K_{ES} \tag{3.3.10}$$

   - The parameters PID_{EAM_i}, N_{EAM_i}, N_Z and time stamp at that instant T_1 are concatenated and its hash value is calculated as A_1

$$A_1 = h\left(PID_{EAM_i}||K_{ES}||N_Z||T_1\right) \tag{3.3.11}$$

   - It then sends a message M_1 to aggregating charge station ACS_i containing PID_{EAM_i}, A_1, N_Z and time stamp T_1.

$$M_1 = \{PID_{EAM_i}, A_1, N_Z, T_1\} \tag{3.3.12}$$

2. At ACS_i:

- The aggregating charge station ACS_i checks the time freshness and generates N_C by taking input a nonce n_c into its PUF.

$$N_C = PUF\left(n_c\right) \tag{3.3.13}$$

- It then computes a parameter N_X by taking XOR of N_C and its shared key K_{AG}.

$$N_X = N_C \oplus K_{AG} \tag{3.3.14}$$

- After that, ACS_i selects its pseudo-identity SID_{ACS_i} (assigned by GS in registration phase). The parameters SID_{ACS_i}, N_X, N_Z, K_{AG} and time stamp at that instant T_2 are concatenated and its hash value is calculated as A_2

$$A_2 = h\left(SID_{ACS_i}||N_X||N_Z||T_2||K_{AG}\right) \tag{3.3.15}$$

- It then sends a message M_2 containing $M_1, SID_{ACS_i}, A_2, N_X$ and its time stamp of that instant T_2 to the grid station GS.

$$M_2 = \{M_1, SID_{ACS_i}, A_2, N_X, T_2\} \tag{3.3.16}$$

3. At GS:

- The GS checks the time freshness and derives N_{EAM_i} by taking XOR of shared key K_{ES} with N_Z.

$$N_{EAM_i} = K_{ES} \oplus N_Z \tag{3.3.17}$$

- It also derives N_C by taking XOR of K_{AG} with N_X.

$$N_C = K_{AG} \oplus N_X \tag{3.3.18}$$

- It verifies A_1 by taking concatenating all the elements, taking hash of it and then comparing that value with the received value.

$$A_1 \stackrel{?}{=} h\left(PID_{EAM_i}||K_{ES}||N_Z||T_1\right) \tag{3.3.19}$$

- Similarly, it verifies the parameter A_2.

$$A_2 \stackrel{?}{=} h\left(SID_{ACS_i}||N_X||N_Z||T_2||K_{AG}\right) \tag{3.3.20}$$

- It checks the pseudo-identities of both EAM_i and ACS_i by decrypting the encrypted values of $(ID_{EAM_i}||R_S)$ and $ID_{ACS_i}||R_A)$ with its secret key K_{GS}.

$$PID_{EAM_i} = D_{K_{GS}}(ID_{EAM_i}||R_S) \tag{3.3.21}$$

$$SID_{ACS_i} = D_{K_{GS}}(ID_{ACS_i}||R_A) \tag{3.3.22}$$

- The GS, then, generates a nonce $R_{S_{new}}$, concatenate it with ID_{EAM_i} and encrypts it with its secret key K_{GS} to update the new pseudo-identity $PID_{EAM_{(new)}}$.

$$PID_{EAM_{(new)}} = E_{K_{GS}}(ID_{EAM_i} || R_{S_{new}}) \tag{3.3.23}$$

- This new pseudo-identity $PID_{EAM_{(new)}}$ is then XORed with shared key between EAM and GS to generate X_{EAM_i}.

$$X_{EAM_i} = PID_{EAM_{(new)}} \oplus K_{ES} \tag{3.3.24}$$

- After this, two parameters A_3 and A_4 are computed as:

$$A_3 = h\left(K_{AG} || SID_{ACS_i} || N_C\right) \tag{3.3.25}$$

$$A_4 = h\left(K_{ES} || PID_{EAM_i} || N_{EAM_i}\right) \tag{3.3.26}$$

- The GS then sends a message M_3 containing A_3, A_4, X_{EAM_i} and time stamp T_3 to the ACS_i.

$$M_3 = \{A_3, A_4, X_{EAM_i}, T_3\} \tag{3.3.27}$$

4. At ACS_i:

- The ACS_i checks the time freshness and verifies A_3 by concatenating shared key between ACS_i and GS *i.e.* K_{AG}, the pseudo-identity

SID_{ACS_i} and its PUF output N_C; taking hash of that value and then comparing it with the value received from GS.

$$A_3 \stackrel{?}{=} h(K_{AG}||SID_{ACS_i}||N_C) \tag{3.3.28}$$

- After that, it sends the message M_4 containing X_{EAM_i}, A_4 and it's time stamp T_4 to the EAM_i.

$$M_4 = \{X_{EAM_i}, A_4, T_4\} \tag{3.3.29}$$

5. At EAM_i:

- The EAM_i checks the time freshness and verifies A_4 by concatenating shared key between EAM_i and GS *i.e.* K_{ES}, the pseudo-identity PID_{EAM_i} and its PUF response N_{EAM_i}; taking hash of that value and then comparing it with the value received from GS.

$$A_4 \stackrel{?}{=} h(K_{ES}||PID_{EAM_i}||N_{EAM_i}) \tag{3.3.30}$$

- After verification, it computes the new pseudo-identity $PID_{EAM_{(new)}}$ by XORing X_{EAM_i} with its shared key K_{ES} and updates it.

$$PID_{EAM_{(new)}} = X_{EAM_i} \oplus K_{ES} \tag{3.3.31}$$

$$PID_{EAM_i} = PID_{EAM_{(new)}} \tag{3.3.32}$$

Table 3.3: Mutual Authentication Phase

GS	ACS_i	EAM_i
		Select: PID_{EAM_i} Generate: nonce n_{eam} Generate: $N_{EAM_i} = \text{PUF }(n_{eam})$ Compute: $N_Z = N_{EAM_i} \oplus K_{ES}$ $A_1 = h(PID_{EAM_i} \vert\vert K_{ES} \vert\vert N_Z \vert\vert T_1)$
	$\xleftarrow{M_1=\{PID_{EAM_i},A_1,N_Z,T_1\}}$	
	$T_2 - T_1 \leq \Delta T$ Generate: nonce n_c Generate $N_C = PUF(n_c)$ Compute: $N_X = N_C \oplus K_{AG}$ Select: SID_{ACS_i} $A_2 = h(SID_{ACS_i} \vert\vert N_X \vert\vert N_Z \vert\vert T_2 \vert\vert K_{AG})$	
$\xleftarrow{M_2=\{M_1,SID_{ACS_i},A_2,N_X,T_2\}}$		
$T_3 - T_2 \leq \Delta T$ Derive: $N_{EAM_i} = K_{ES} \oplus N_Z$ Derive: $N_C = K_{AG} \oplus N_X$ Verify: $A_1?, A_2?, PID_{EAM_i}?, SID_{ACS_i}?$ $PID_{EAM_i} = D_{K_{GS}}(ID_{EAM_i} \vert\vert R_S)$ $SID_{ACS_i} = D_{K_{GS}}(ID_{ACS_i} \vert\vert R_A)$ Generate: nonce $R_{S_{new}}$ Update: $PID_{EAM_{(new)}} = E_{K_{GS}}(ID_{EAM_i} \vert\vert R_{S_{new}})$ $X_{EAM_i} = PID_{EAM_{(new)}} \oplus K_{ES}$ $A_3 = h(K_{AG} \vert\vert SID_{ACS_i} \vert\vert N_C)$ $A_4 = h(K_{ES} \vert\vert PID_{EAM_i} \vert\vert N_{EAM_i})$		
$\xrightarrow{M_3=\{A_3,A_4,X_{EAM_i},T_3\}}$		
	$T_4 - T_3 \leq \Delta T$ Verify: $A_3 \stackrel{?}{=} h(K_{AG} \vert\vert SID_{ACS_i} \vert\vert N_C)$	
	$\xrightarrow{M_4=\{X_{EAM_i},A_4,T_4\}}$	
		$T_5 - T_4 \leq \Delta T$ Verify: $A_4 \stackrel{?}{=} h(K_{ES} \vert\vert PID_{EAM_i} \vert\vert N_{EAM_i})$ Compute and Update: $PID_{EAM_{(new)}} = X_{EAM_i} \oplus K_{ES}$ $PID_{EAM_i} = PID_{EAM_{(new)}}$

3.4 Summary

This chapter gave an overview and discussed the V2G network model and threat model. It also defined the security goals as well as security assumptions for the proposed scheme. It also put forward a novel user key exchange authentication scheme for V2G based frameworks explaining all three phases of registration of electric automobile and aggregating charge station with grid station as well the mutual authentication phase in detail. The chapter 4 discusses the security analysis of the proposed scheme.

Chapter 4

Security Analysis

4.1 Overview

The security feature and robustness of our enhanced suggested authentication system are scrutinised and analysed. We analyse adversarial model in terms of security measures of our suggested system in the act of adversarial model, which we briefly mentioned in chapter 1. In this chapter, we looked at how powerful our suggested security protocol is against all known adversary security threats. Additionally, we compared and discussed the security needs of our proposed security protocol. We used BAN-Logic and ProVerif for formal security analysis, and informal security analysis was tested against several security threats.

4.2 Formal Security Analysis

4.2.1 Proverif

ProVerif is an automation tool that may be used to evaluate and analyze different security features of authentication, anonymity and accessibility etc. ProVerif primarily checks the designed security protocol's accuracy and robustness [62]. Message authentication code MAC, digital signatures, encryption & decryption, elliptic curve cryptographic functions, hash functions as well as many other cryptographic functions are all supported by ProVerif [63].

In our presented scheme for user key exchange mutual authentication, we have communication carried out via two different channels:

- Private channel (ChSec): This is a secure channel where the registration of EAM_i and ACS_i is carried out with the GS.
- Public Channel (ChPub): This is a public channel used for the mutual authentication of all entities *i.e.* AEM_i, ACS_i and GS involved in a V2G network.

The GS is mutually authenticated by ACS_i and EAM_i. The EAM_i is authenticated with GS through ACS_i and ACS_i is authenticated with both EAM_i and GS. All these entities *i.e.* AEM_i, ACS_i and GS generate and verify different parameters in the mutual authentication phase. These include different nonces, time stamps and messages etc. The pseudo-identities generated by GS for EAM_i and ACS_i are PID_{EAM_i} and SID_{ACS_i} respectively. The secret key of GS is K_{GS}.

The GS shares secret shared key K_{ES} with EAM_i and secret shared key K_{AG} with ACS_i which are generated and delivered to EAM_i and ACS_i in their respective registration phases. Constructors for the XOR, Hash, Concatenation, encryption, and decryption functions are specified and the results of the ProVerif code for our proposed method are presented below.

4.2.1.1 Proverif Code

The proverif code for our proposed scheme is described below:

```
(* --------- Channels ----------*)
free ChSec:channel [private]. (*secure channel *)
free ChPub:channel. (*public channel *)


(*----------- Constants and Variables ---------*)
free PIDEAMi : bitstring [private].
free Neam : bitstring.
free PUF : bitstring.
free Nz : bitstring.
free Kes : bitstring.
free M1 : bitstring.
free T1 : bitstring.
free T2 : bitstring.
free T3 : bitstring.
free T4 : bitstring.
```

```
free T5 : bitstring.

free Nc : bitstring.

free nc: bitstring.

free Nx : bitstring.

free Kag : bitstring.

free SIDacsi : bitstring[private].

free M2 : bitstring.

free A1 : bitstring.

free A2 : bitstring.

free A3 : bitstring.

free A4 : bitstring.

free Neami : bitstring.

free Dkgs : bitstring.

free IDacsi : bitstring.

free Ra : bitstring.

free RS : bitstring.

free RSnew : bitstring.

free Xeamnew : bitstring.

free PIDeamnew : bitstring.

free Kes : bitstring.

free XEAMi : bitstring[private].

free M3 :bitstring.
```

```
(*========Constructors=======*)

fun h(bitstring) : bitstring.

fun h2(bitstring,bitstring): bitstring.

fun Concat(bitstring,bitstring) : bitstring.

fun XOR(bitstring,bitstring) : bitstring.

fun Ekgs(bitstring) : bitstring.

fun Dkgs(bitstring) : bitstring.


(*======Equations=======*)

 equation for all a : bitstring, b : bitstring; XOR(XOR(a,b),b)=a.
```

In ProVerif code, an electric automobile EAM_i selects its pseudo-identity PID_{EAM_i} and generates some parameters using its PUF and sends them over to ACS_i. The code is processed as:

```
(*---------------Authentication---------------------*)

(*-------------EAMi--------------*)

let PIDEAMi=

event start_EAMi(PIDEAMi);

let xNz=XOR(Neami,Kes) in

let xA1=h(Concat(PIDEAMi,(Kes, Nz, T1)) in

let xFi=h(XOR(CIDi,(Ti,DIDi))) in


out(ChPub,M1=(PIDEAMi,A1,Nz,T1));
```

```
in(ChPub,xM4=(Xeami:bitstring ,xA4 :bitstring , xT4:bitstring));
let xA4=h(Concat(Kes,(PIDEAMi, Neami)) in
let xxPIDeamnew=XOR(Xeami,Kes) in
let PIDEAMi=xxPIDeamnew in
event end_EAMi(PIDEAMi)
else
0.
```

At the aggregating charge station ACS_i end, ACS_i also chooses its pseudo-identity SID_{ACS_i} and the code processes as follows:

```
(*--------------- Authentication---------------------*)
(*======*ACS*=======*)
let ACS=
event start_ACS(IDGS);
let xNc= nc in
let xNx=XOR(Nc,Kag) in
in(ChPub,(PIDEAMi:bitstring,xA1:bitstring,xNz:bitstring,xT1:bitstring));
let xCIDi=h(Concat(IDi,(h(x)))) in
let xA2=h(Concat(SIDacsi,(Nx,CIDi,Nz,T2,Kag))) in
out(ChPub,M2=(M1 ,SIDacsi, xA2,xNx,T2));
in(ChPub,(xA3:bitstring,xA4:bitstring,XEAMi:bitstring,xT3:bitstring));
if A3=h(Concat(Kag,(SIDacsi,Nc)) then
```

```
out(ChPub,M4=(Xeami,A4,T4));
 event end_ACS(SIDacsi)
else 0.
```

The authentication mechanism at GS is carried out as follows:

```
(*--------------- Authentication---------------------*)
(*======*GS*=======*)
let GS=
event start_GS(IDGS);
let xNeami=XOR(Kes,Nz) in
let xxNc=XOR(Kag,Nx) in
if A1,A2,PIDEAMi,SIDcsai then
let xxPIDEAMi=Dkgs(Concat(IDEAMi,Rs) in
let xxSIDcsai=Dkgs(Concat(IDCSAi,Ra) in
let xPIDeaminew=Ekgs(Concat(IDEAMi,Rs) in
let xXeami=XOR(xPIDeaminew,Kes) in
let xxA3= h(Concat(Kag,(SIDcsai, Nc)) in
let xxA4= h(Concat(Kes,(PIDeami, Neami)) in
in(ChPub,(xxM1:bitstring,xSIDcsai:bitstring,xxNx:bitstring,
xA2:bitstring,xxT2:bitstring));
out(ChPub,M3=(A3,A4,Xeami,T3));
event end_GS(IDGS)
else 0.
```

The parallel execution of protocol is as shown below:

```
process ( (!pGS) | (!pCSA) | (!pEAMi))
```

The following mentioned queries are used to verify authentication characteristics for the proposed protocol:

```
(*-------Queries------*)
query PIDEAMi:bitstring; inj-event(end_EAMi(PIDEAMi)) ==>
inj-event(start_EAMi(PIDEAMi)).
query SIDcsai:bitstring; inj-event(end_CSA(SIDcsai)) ==>
inj-event(start_CSA(SIDcsai)).
query XEAMi:bitstring; inj-event(end_GS(XEAMi)) ==>
inj-event(start_GS(XEAMi)).
query attacker(PIDEAMi).
```

Six different events are employed in proposed Proverif code *i.e* electric automobile EAM_i event (begin/end), aggregating charge station ACS_i event (begin/end) and grid station GS event (start/end).

```
(*=====*Events*=====*)
event start_EAMi(bitstring).
event end_EAMi(bitstring).
event start_ACS(bitstring).
event end_ACS(bitstring).
event start_GS(bitstring).
```

```
event end_GS(bitstring).
```

4.2.1.2 Proverif Results

After the compilation of our proposed protocol ProVerif code we get the following results:

```
Completing...
Starting query inj-event(end_EAMi(PIDEAMi_4)) ==>
inj-event(start_EAMi(PIDEAMi_4))
goal reachable: attacker(Xeami_3) && attacker(xA4_3) && attacker(xT4_1)
&& begin(@p_act(@occ42_1,(Xeami_3,xA4_3,xT4_1))) &&
begin(start_EAMi(IDEAMi[]),@occ35_1) ->
end(@occ46_1,end_EAMi(IDEAMi[]))
The 1st, 2nd, 3rd hypotheses occur before the conclusion.
The 4th, 5th hypotheses occur strictly before the conclusion.
Abbreviations:
@occ46_1 = @occ46[xT4 = xT4_1,xA4_1 = xA4_3,Xeami_2 = Xeami_3,!1 = @sid]
@occ42_1 = @occ42[!1 = @sid]
@occ35_1 = @occ35[!1 = @sid]
RESULT inj-event(end_EAMi(PIDEAMi_4)) ==>
inj-event(start_EAMi(PIDEAMi_4)) is true.

-- Query inj-event(end_ACS(SIDacsi_1)) ==>
inj-event(start_ACS(SIDacsi_1)) in process 1
```

```
Translating the process into Horn clauses...

Completing...

Starting query inj-event(end_ACS(SIDacsi_1)) ==>

inj-event(start_ACS(SIDacsi_1))

RESULT inj-event(end_ACS(SIDacsi_1)) ==>

inj-event(start_ACS(SIDacsi_1)) is true.

-- Query inj-event(end_GS(XEAMi_2)) ==>

inj-event(start_GS(XEAMi_2)) in process 1

Translating the process into Horn clauses...

Completing...

Starting query inj-event(end_GS(XEAMi_2)) ==>

inj-event(start_GS(XEAMi_2))

RESULT inj-event(end_GS(XEAMi_2)) ==>

inj-event(start_GS(XEAMi_2)) is true.

-- Query not attacker(PIDEAMi[]) in process 1

Translating the process into Horn clauses...

Completing...

Starting query not attacker(PIDEAMi[])

RESULT not attacker(PIDEAMi[]) is true.


Verification summary:


Query inj-event(end_EAMi(PIDEAMi_4)) ==>

inj-event(start_EAMi(PIDEAMi_4)) is true.
```

```
Query inj-event(end_CSA(SIDcsai_1)) ==>
inj-event(start_CSA(SIDcsai_1)) is true.
Query inj-event(end_GS(XEAMi_2)) ==>
inj-event(start_GS(XEAMi_2)) is true.
Query not attacker(PIDEAMi[]) is true.
```

The results presented proves that all main processes of our proposed scheme are carried out successfully with no issues with initializing as well as their termination and that our proposed protocol for V2G based frameworks achieve the defined security goals of authentication, secrecy, anonymity and communication integrity.

4.2.2 BAN Logic

We have utilized Burrows Abadi-Needham (BAN) logic [64] to validate mutual authentication for our proposed scheme. The rationale of the BAN logic is based on a set of principles that establish the security scheme characteristics [65]. Details about BAN logic's different notations, analogous forms, hypotheses, and demonstrations are presented in table 4.1.

Different goals must be defined in order to assess the security of a protocol using BAN logic. Based on BAN logic, eight distinct goals have been defined for our proposed scheme and are listed below:

- Goal 1: $ACS_i| \equiv EAM_i \overset{PID_{EAM_i}}{\longleftrightarrow} ACS_i$
- Goal 2: $ACS_i| \equiv EAM_i| \equiv EAM_i \overset{PID_{EAM_i}}{\longleftrightarrow} ACS_i$

Table 4.1: BAN Logic Notations

Notations	Description
$P\mid\equiv X$	P Believes that X
$P \lhd X$	P Sees that X
$P\mid\sim X$	P once said X
$P \Rightarrow X$	P have total jurisdiction on X
$\#(X)$	X is updated and fresh
(X,Y)	X, Y is component of formula(X,Y)
$< X >_Y$	X is combine with Y
$(X)_K$	Hash of message X using a key K
$P \stackrel{K}{\longleftrightarrow} Q$	P and Q are using shared key K for communication process
PID_{EAM_i}	Session key PID_{EAM_i} is used one time in a current section
$\frac{P\mid\equiv P \stackrel{K}{\longleftrightarrow} Q . p \lhd <X>_K}{P\mid\equiv Q\mid\sim X}$	Message-Meaning rule
$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$	Freshness-conjuncatenation rule
$\frac{P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	Nonce-verification rule
$\frac{P\mid\equiv Q\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$	Jurisdiction rule
$P\mid\equiv X$	P believes X

- Goal 3: $GS\mid\equiv ACS_i \stackrel{PID_{EAM_i}}{\longleftrightarrow} GS$

- Goal 4: $GS\mid\equiv ACS_i\mid\equiv ACS_i \stackrel{PID_{EAM_i}}{\longleftrightarrow} GS$

- Goal 5: $ACS_i\mid\equiv GS \stackrel{PID_{EAM_i}}{\longleftrightarrow} ACS_i$

- Goal 6: $ACS_i\mid\equiv GS\mid\equiv GS \stackrel{PID_{EAM_i}}{\longleftrightarrow} ACS_i$

- Goal 7: $EAM_i\mid\equiv ACS_i \stackrel{PID_{EAM_i}}{\longleftrightarrow} EAM_i$

- Goal 8: $EAM_i\mid\equiv ACS_i\mid\equiv ACS_i \stackrel{PID_{EAM_i}}{\longleftrightarrow} EAM_i$

The security analysis employing BAN logic has been separated into three stages to meet the objectives stated above. Part 1 depicts the theoretical form of the protocol, which is verified in Part 3, whereas Part 2 shows evaluates the protocol using hypotheses.

Part 1: It depicts the theoretical form of the protocol.

- M1: $EAM_i \rightarrow ACS_i : PID_{EAM_i}, A_1, N_Z, T_1$

- M2: $ACS_i \rightarrow GS : M_1, SID_{ACS_i}, A_2, N_X, T_2$

- M3: $GS \rightarrow ACS_i : A_3, A_4, X_{EAM_i}, T_3$

- M4: $ACS_i \rightarrow EAM_i : X_{EAM_i}, A_4, T_4$

Part 2: It presents the hypotheses used for the evaluation of the proposed protocol.

- H1: $EAM_i| \equiv \#N_{eam}$

- H2: $ACS_i| \equiv \#N_c$

- H3: $GS| \equiv \#R_{S_new}$

- H4: $ACS_i| \equiv GS \Rightarrow R_{S_new}$

- H5: $ACS_i| \equiv EAM_i \Rightarrow N_{eam}$

- H6: $GS| \equiv ACS_i \Rightarrow N_c$

- H7: $GS| \equiv EAM_i \Rightarrow N_{eam}$

- H8: $EAM_i| \equiv GS \Rightarrow R_{S_new}$

- H9: $EAM_i| \equiv ACS_i \Rightarrow N_c$

Part 3: The following is an elaborate analysis of the suggested protocol, obtained using BAN logic assumptions and rules:

M1: $EAM_i \rightarrow ACS_i : PID_{EAM_i}, A_1, N_Z, T_1$; where T_1 is the timestamp of the EAM_i.

The following is achieved through the seeing rule:

- F1: $ACS_i \triangleleft PID_{EAM_i}, A_1, N_z, T_1$

The following can be obtained according to the F1 and the message-meaning rule:

- F2: $ACS_i | \equiv EAM_i | \sim N_{eam}$

By the use of Freshness-conjuncatenation rule and F2, it is achieved:

- F3: $ACS_i | \equiv EAM_i | \equiv N_{eam}$

With the use of jurisdiction rule and F3, it is achieved:

- F4: $ACS_i | \equiv N_{eam}$

Using F4 and session key rule, it is achieved:

- F5: $ACS_i | \equiv EAM_i \overset{PID_{EAM_i}}{\longleftrightarrow} ACS$ Goal 1

By the utilizing nonce-verification rule and F5, we obtain:

- F6: $ACS_i | \equiv EAM_i | \equiv EAM_i \overset{PID_{EAM_i}}{\longleftrightarrow} ACS_i$ Goal 2

M2: M2: $ACS_i \rightarrow GS : M_1, SID_{ACS_i}, A_2, N_X, T_2$ where T_2 is the timestamp of ACS_i.

According to the seeing rule, we have:

- F7: $GS \triangleleft M1, SID_{ACS_i}, A_2, N_X, T_2$

By the use of message-meaning rule and F7, we get:

- F8: $GS| \equiv ACS_i| \sim N_C$

The utilization of Freshness-conjuncatenation rule and F8 shows:

- F9: $GS| \equiv ACS_i| \equiv N_C$

By application of the jurisdiction rule and F9, we get:

- F10:$GS| \equiv N_C$

By F10 and the session key rule:

- F11: $GS| \equiv ACS_i \overset{PID_{EAM_i}}{\longleftrightarrow} GS$ Goal 3

By making use of nonce-verification rule and F11, we obtain:

- F12: $GS| \equiv ACS_i| \equiv ACS_i \overset{PID_{EAM_i}}{\longleftrightarrow} GS$ Goal 4

M3: $GS \rightarrow ACS_i : A_3, A_4, X_{EAM_i}, T_3$ where T_3 is the timestamp of GS.

By making use of the seeing-rule, we acquire:

- F13: $ACS_i \triangleleft A_3, A_4, X_{EAM_i}, T_3$

By the use of message-meaning rule and F13, we get:

- F14: $ACS_i| \equiv GS| \sim N_C$

The utilization of Freshness-conjuncatenation rule and F14 shows:

- F15: $ACS_i| \equiv GS| \equiv N_C$

By application of the jurisdiction rule and F15, we get:

- F16: $ACS_i| \equiv N_C$

By F16 and the session key rule:

- F17: $ACS_i| \equiv GS \overset{PID_{EAM_i}}{\longleftrightarrow} ACS_i$. Goal 5

By making use of nonce-verification rule and F17, we obtain:

- F18: $ACS_i| \equiv GS| \equiv GS \overset{PID_{EAM_i}}{\longleftrightarrow} ACS_i$ Goal 6

M4: $ACS_i \rightarrow EAM_i : X_{EAM_i}, A_4, T_4$ where T_4 is the timestamp of ACS_i.

By making use of the seeing-rule, we acquire:

- F19: $EAM_i \triangleleft X_{EAM_i}, A_4, T_4$

By the use of message-meaning rule and F19, we get:

- F20: $TEAM_i| \equiv ACS_i| \sim R_{new}$

The utilization of Freshness-conjuncatenation rule and F20 shows:

- F21: $EAM_i| \equiv ACS_i| \equiv R_{new}$

By application of the jurisdiction rule and F21, we get:

- F22: $EAM_i| \equiv R0_{new}$

By F22 and the session key rule:

- F23: $EAM_i| \equiv ACS_i \overset{PID_{EAM_i}}{\longleftrightarrow} EAM_i$ Goal 7

By making use of nonce-verification rule and F23, we obtain:

- F24: $EAM_i| \equiv ACS_i| \equiv ACS_i \overset{PID_{EAM_i}}{\longleftrightarrow} EAM_i$ Goal 8

We have demonstrated by utilization the BAN logic; all entities in our network model *i.e.* EAM_i, ACS_i and GS were able to initiate and complete a secure session key agreement and thus, establish mutual authentication.

4.3 Informal Security Analysis

We will discuss an informal security analysis by highlighting the security features of our proposed mutual authentication protocol in the following subsections.

4.3.1 Mutual Authentication

The proposed protocol provides mutual authentication among all the entities *i.e.* EAM_i, ACS_i and GS. Different parameters are generated and verified at different stage of the protocol *i.e.* A_1 & A_2 generated by EAM_i and ACS_i respectively are verified by GS and A_3 & A_4 generated by GS are verified by ACS_i and EAM_i respectively.

4.3.2 Identity Protection

One of the fundamental security grounds for communication schemes is its feature of identity protection of its users. During the registration phases, the pseudo identities are created for both EAM_i and ACS_i that play a pivotal role during the authentication phase. The original identities of both are sent over a secure and private channel that can not be intercepted. Also, to deduce the pseudo-identities from original identities is an extremely difficult task for an adversary and an adversary has no means of knowing the entities even if he captures the messages containing pseudo-identities of either EAM_i and ACS_i.

4.3.3 Forward & Backward Secrecy

The information communicated in a session is not prone to tracking, hacking or utilisation by an attacker in any way to exploit any vulnerability in the current, previous, or future authentication sessions between the GS and EAM_i for proposed scheme to run successfully. Even if the identities PID_{EAM_i} and / or SID_{ACS_i} are somehow dropped in the proposed protocol's current session; prior or subsequent sessions are unaffected. It is made possible due to the fact that the each sessions is initiated by a new pseudo identity of EAM_i which is constantly updated with each new session. The suggested protocol for the V2G network ensures backward and forward secrecy in this way.

4.3.4 Scalability

All the cryptographic functions in the proposed functions are lightweight and no exhaustive primitive is employed. The generation and verification of different parameters at different entities involve simple operations of concatenations, hash and XOR. Only the GS performs AES encryption and decryption at its end while the authentication phase is in progress. This property makes our protocol very scalable in nature.

4.3.5 Resistance against Eavesdropping / Message Analysis Attack

Security against attacks targeting confidentiality and privacy of a communication session is a vital feature of our protocol. Every message in our scheme's mutual authentication phase contains of parameters that are either XORed or digests of other variable bit strings *e.g.* A_1, A_2, A_3 and A_4 are digests of multiple concatenated parameters and M_1, M_2, M_3 and M_4 contain digests or pseudo-identities. There is no possibility of an adversary getting any actual or useful information even if he manages to sniff and / or capture some of the messages during an ongoing session.

4.3.6 Resistance against Impersonation Attack

Both the EAM_i and ACS_i are assigned their pseudo-identities PID_{EAM_i} and SID_{ACS_i} respectively during their registration phase that are used for the mutual authentication and are updated for the next session. Along with this, all EAM_i and ACS_i have their own unique PUF that create a unique parameter N_{EAM_i} and N_C respectively that can not be generated through any other means. The rest of the parameters containing digests are verified at GS. Since hash is a one-way cryptographic operation bearing collision resistant property, the chances of an adversary to replicate the verification elements is very low. If he manages to inject a message by sniffed pseudo-identity of either EAM_i or ACS_i, it is highly unlikely to carry out the rest of operations and maintain the timestamps to be able to get verified by the GS. Thus, our proposed protocol is resistant to impersonation attack.

4.3.7 Resistance against Message Modification Attack

The proposed protocol has fresh timestamps for every node in the mutual authentication phase. Any modification of a message by an adversary will require sniffing, capture and altering the message in such a manner that the time freshness at any node doesn't exceed the limit after which the session is terminated and all the messages received after that time frame or with the time stamp exceeding that limit are discarded. Since its very hard for an adversary to carry this out in Probabilistic Polynomial Time (PPT), the scheme is impervious to message modification attack and provides data integrity.

4.3.8 Resistance to Replay Attack

Since the mutual authentication is carried out on a public channel, it is possible for an adversary to capture the messages being sent and received from one entity to another. The adversary can use these message to initiate the authentication at a later time. However, in our proposed scheme all the messages M_1, M_2, M_3 and M_4 contain fresh time stamps T_1,T_2,T_3 and T_4 from EAM_i,ACS_i,GS and EAM_i respectively and after every message is received, the first step is to check for time freshness. Any message received with an older timestamp is discarded and session is terminated. Aso, other parameters in the messages M_1, M_2, M_3 and M_4 are freshly generated for each new session so the adversary can not generate them again later and reuse them to initiate a false authentication session. Thus, our presented scheme provides resistance against replay attack.

4.3.9 Resistance to Man in the Middle (MITM) Attack

An adversary can act as an imposter between EAM_i and ACS_i or between ACS_i and GS to launch a MITM attack. In our proposed protocol, both EAM_i and ACS_i have embedded PUFs in their hardware that generate parameters N_{EAM_i} and N_C respectively that can not be replicated by any cryptographic algorithms. Also, multiple parameters containing different elements from all entities are verified at every node and since it has already been established that an adversary can not modify message nor inject any other information in any ongoing session; this proves that our proposed scheme is impervious to MITM attack.

4.3.10 Session Key Security

During registration phase of our proposed protocol, the GS generates shared session keys K_{ES} and K_{AG} for EAM_i and ACS_i respectively. These keys are generated by taking a nonce value, identity of GS and identities of EAM_i and ACS_i and some cryptographic operations are performed including concatenation of two parameters, calculating hash values and taking XORs. These keys are then sent to their respective entities through a message over a secure private channel. During the mutual authentication phase, these keys are never sent openly on public channel rather their digests (along with other concatenated parameters) are shared in messages so that they can be verified by other entities. The session keys are never exposed and can not be intercepted or captured by any adversary in our protocol providing adequate session key security.

4.3.11 Resistance against Traceability

During the registration phases, the pseudo identities PID_{EAM_i} and SID_{ACS_i} are created for both EAM_i and ACS_i respectively that play a pivotal role in mutually authenticating these entities with the GS. After every session, the pseudo-identity of EAM_i is updated. The use of a new pseudo-identity of EAM_i for every session renders it impossible to track the transactions of an electric automobile with respect to its identity. An adversary can not gain any information about behaviour or communication history of a certain EAM_i due to constantly changing pseudo-identities. Even if an adversary is able to map one identity to a specific

EAM_i, it still won't be able to track it because the identity $i.e$ (pseudo identity $PID_{EAM_i} = PID_{EAM_{new}}$) would be different for that very EAM_i in the very next session. In this way, our proposed protocol gives security against risks associated with traceability issues.

4.3.12 Resistance to DOS Attack

The protocol is based on mutual authentication and constant up-gradation of pseudo-identities, which are properly encrypted and communicated for every transaction, rather than any random key that is responsible for EAM_i or ACS_i authentication or verification. At any point, where a verification of a single parameter is false, the session is terminated. As a result, the suggested protocol is impervious to DoS attack.

4.3.13 Physical Security

An adversary may seek to attain physical access to an electric automobile EAM_i or an aggregating charge station ACS_i and then strive to retrieve the stored parameters in that entity's device memory. Even though, it is assumed that gaining access to EAM_i and GS as they possess ample hardware protection is harder than accessing ACS_i which are installed in open areas. Our proposed scheme makes use of embedded PUFs in hardware of both EAM_i or ACS_i whose communication with the device's microcontroller is secure [66] deletes all the parameters after the session is terminated and for the next session, all are freshly generated so even if an adversary is successful in gaining access to ACS_i or EAM_i device memory, it will yield no data, making the proposed protocol protected against physical security risks.

4.4 Summary

This chapter presented the security analysis a novel user key exchange authentication (NUKA) scheme for V2G based frameworks. The formal security analysis was carried out by Proverif and BAN Logic. Security analysis by Proverif showed that our protocol achieves the defined security goals of authentication, secrecy, anonymity and communication integrity. By BAN Logic, we presented the validation of mutual authentication in our protocol. The informal security analysis discussed the security features of the proposed protocol as well as the the resistance that it provides against known attacks. The performance analysis will be presented in Chapter 5 in detail.

Chapter 5

Performance Analysis

5.1 Overview

This chapter discusses the performance analysis of the proposed protocol for user key exchange authentication scheme for V2G frameworks. The analysis is discussed in three sections. First, a comparison is drawn on the basis of well defined security attributes and proved that the proposed scheme features the maximum security traits. Secondly, computational overhead of different existing schemes as well as ours is presented in detail and analyzed for its complexity. Lastly, performance analysis is carried out in terms of computational time that it takes to run a protocol and is represented graphically.

5.2 Security Attributes Comparison

In this section, we will make comparisons of our proposed scheme (PS) with some of the existing literature with respect to its security attributes (SAs) and the resistance it exhibits against some known vulnerabilities and risks. The security attributes defined for our comparison are as follows:

- SA_1: Mutual Authentication
- SA_2: Identity Privacy
- SA_3: Scalability
- SA_4: Message Confidentiality / Resistance to Eavesdropping
- SA_5: Security against Impersonation Attack
- SA_6: Message Integrity / Resistance to Message Modification Attack
- SA_7: Security against Replay Attack
- SA_8: Security against MITM Attack
- SA_9: Session Key Security
- SA_{10}: Security against Traceability
- SA_{11}: Resistance to DOS Attack
- SA_{12}: Physical Security
- SA_{13}: Formal Security Proof

The comparison is demonstrated in table 5.1 with ✓depicting the presence of that attribute and blank space implying either no provision or negligence of that attribute in the corresponding protocol.

Table 5.1: Comparison of Security Attributes

SA	SA_1	SA_2	SA_3	SA_4	SA_5	SA_6	SA_7	SA_8	SA_9	SA_{10}	SA_{11}	SA_{12}	SA_{13}
[33]	✓	✓		✓	✓	✓	✓	✓	✓				✓
[34]	✓	✓		✓		✓	✓	✓	✓				
[36]	✓	✓	✓										
[38]	✓			✓	✓	✓	✓	✓					✓
[37]	✓	✓						✓	✓				
[43]		✓		✓	✓	✓	✓	✓	✓				
[67]	✓	✓	✓				✓				✓		
[55]	✓	✓		✓	✓	✓	✓	✓	✓				
[56]	✓	✓					✓						
[57]	✓	✓					✓						
[58]	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓
[61]	✓		✓	✓		✓	✓				✓	✓	✓
PS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

As evident from table 5.1, mutual authentication is a pivotal feature for all schemes except for [43]. Scalability and lightweight protocol is proposed by [36, 58, 61, 67] as well as our proposed scheme *i.e.* NUKA. The authors in [33, 38, 58, 61] have presented a formal security proof of their scheme. NUKA also claims its security attributes through formal and informal security proofs. Risk to identity privacy is a major vulnerability in [38, 58, 61]. The protocols in [36, 37] are prone to eavesdropping and message modification whereas [56, 57, 67] lack the attribute of data confidentiality as well as integrity. All the schemes discussed in [34, 36, 37, 56, 57, 61, 67] transmit user identity openly on a public challenge making an impersonation and MITM attack possible for the adversary. Similarly, absence of any timestamp parameter in [36] and [37] makes them prone to replay attack. The security attribute of session key security is not supported by [36, 38, 56, 57, 67] and [61]. Resistance against DOS attack is addressed in [61, 67] and NUKA by ensuring the termination of session as soon as failure of a single verification occurs. NUKA and [58, 61] have PUFs embedded in their entities' hardware. Since no security parameter is stored on device's memory and also, all communication between PUF and device's microcontroller is tamper-resistant; these key features make these schemes impervious to physical security threats. All the protocols except for our proposed scheme NUKA are susceptible to threats associated with lack of anonymity and can be exploited by traceability attack. We conclude that our proposed scheme NUKA provides maximum security attributes and provides an ultra-lightweight scheme for V2G based frameworks.

5.3 Computation Overhead

The computation overhead of NUKA along with that of other state of the art schemes is discussed in this section. The overhead is mentioned for one session *i.e.* an electric vehicle getting authenticated by the grid station. Different cryptographic operations are listed including XOR, scalar and ECC point multiplication & addition, exponential functions, bilinear pairings, hashes, signing, symmetric & public encryption / decryption, MAC / HMAC, PUF and Chebyshev polynomial computation upon which a comparison is drawn in table 5.2.

Our proposed protocol NUKA makes use of 6 XORs, 6 hash functions, 1 symmetric encryption, 2 symmetric decryption and 2 PUF operations. Our proposed protocol offers scalability as no heavyweight algorithms are employed as is the case with

Table 5.2: Computation Overhead Comparison

Operations	[34]	[36]	[38]	[43]	[50]	[58]	[67]	[41]	[56]	[57]	[61]	PS
$\oplus$, x, +, exponential functions	81	36	9	-	37	33	-	2	7	4	12	6
Pairing	19	-	2	-	2	-	-	2	-	-	-	-
ECC point multiplication	-	-	-	-	-	-	-	5	18	-	-	-
Hash *h()*	6	9	10	4	16	-	14	12	4	14	14	6
Signing	-	-	2	4	-	-	-	-	-	-	-	-
Symmetric Encryption / Decryption	-	2	2	12	-	6	-	-	-	2	-	3
Public Key Encryption / Decryption	-	-	-	8	-	-	-	-	-	-	-	-
MAC/HMAC	7	4	-	-	-	8	-	-	-	-	-	-
PUF	-	-	-	-	-	2	-	-	-	-	2	2
Chebyshev polynomial computation	-	-	-	-	-	-	-	-	-	8	-	-

[41, 56] and [57]. Even though [67] uses only 14 hashes, their scheme is susceptible to many security threats and does not provide physically security. The schemes of [58] and [61] also have embedded PUF in their systems but even though [58] doesn't make use of hashes, it has 33 cryptographic functions (XOR, scalar multiplications etc,), 6 symmetric encryption / decryption, and 8 MAC / HMAC along with 2 PUF functions. Similarly, in [61], 14 multiple cryptographic functions along with 14 hashes and 2 PUF functions are used which, even though being lightweight than the others, still are computationally extensive than NUKA. Thus, we can deduce that the tradeoff challenge between efficiency and security features has been addressed by NUKA productively as evident from table 5.1 and table 5.2.

5.4 Performance Comparison

The execution time of our scheme (NUKA) along with some of the discussed schemes in chapter 2 are presented in this section. The system specifications used to carry out the computation of our scheme are shown in table 5.3.

Table 5.3: System's Specifications

Component	Specifications
Operating System	Ubuntu 20.04.2 LTS
OS type	64-bit
Processor	Intel Core i3-4005U CPU AT 1.70GHz x 4
RAM	6.1GB; 5.8GB available

Since it was discussed in chapter 3 that GS has far more computational capabilities than EAM and ACS thus, only performance analysis is carried out for EAM and ACS only. The execution times of multiple cryptographic functions, where unavailable, have been taken as reference from [68]. In addition, we used the execution time of a 128-bit Arbiter PUF on the AT91SAM3X8E micro-controller board [69] to calculate the execution time of a PUF function. Table 5.4 shows the execution time (in milliseconds) of different protocols at their electric automobile EAM nodes.

5.4.1 Execution Time Comparison of PUF Based Schemes

The graphical comparison of execution time for PUF based schemes is shown in figure 5.4. In [58], at its electric vehicle node, the operations carried out are 1 PUF function, 1 MAC, 3 nonlinear cryptographic functions and 6 XOR. 1 symmetric decryption, 14 XOR, 2 MAC and multiple nonlinear cryptographic functions (ac-

Table 5.4: Execution Time at EAM

Scheme	Time (ms)
[49]	7.464
[50]	3.072
[34]	3.682
[36]	2.022
[56]	192.030
[38]	8.932
[55]	3.950
[58]	0.845
[67]	0.396
[57]	52.320
[61]	0.117
NUKA	0.071

cording to number of challenge response pairs) are carried out at aggregator's end. The execution time for electric vehicle and aggregator is 2.18 ms and 1.06 ms respectively. The EV node in [61] computes only 3 hashes while charge station carries out 4 hashes and 2 PUF functions in 0.118 ms and 0.366 ms respectively. In our proposed protocol (NUKA), the EAM as well as ACS compute 2 hashes and perform 1 PUF based operation and their time is same as 0.071 ms. It is evident from the graph that our scheme outperforms the other two PUF based authentication schemes in terms of operational capacity as well as computational efficiency.

5.5 Summary

This chapter presented the performance analysis of the proposed protocol for user key exchange authentication scheme for V2G frameworks. The analysis was spread over three sections. First, a comparison was made based on well-defined security

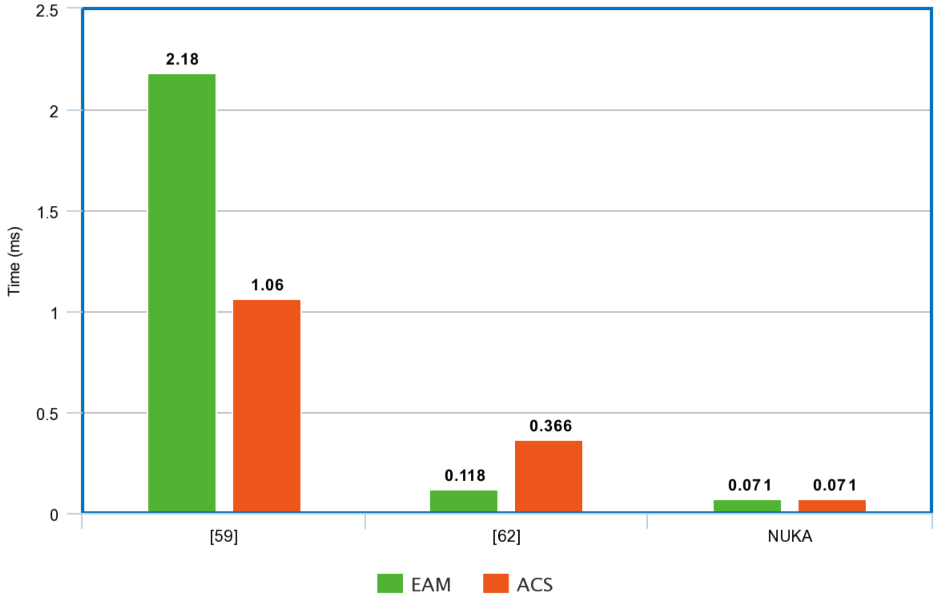


Figure 5.1: Execution Time Comparison of PUF Based Schemes

criteria, and it was demonstrated that the suggested protocol has the highest level of security. Second, the computational overhead of several state of the art schemes, as well as our own, was provided in detail and its complexity was assessed. Finally, performance analysis was carried out in terms of the amount of time it takes to run a protocol and a comparison was presented graphically. In terms of operational capacity and computational efficiency, our approach outperforms the other schemes in general and PUF-based authentication techniques specifically. Chapter 6 will discuss some future prospects of this research and conclude the study.

Chapter 6

Conclusion and Future Horizons

6.1 Overview of Research

Traditional fuel based automobiles are being replaced swiftly with other source oriented vehicles such as solar and electric powered etc. Electric automobiles (EAMs) are one of the emerging and accessible technologies in the transportation sector to decrease CO_2 eruptions and oil demand making up the basis of vehicle to grid (V2G) networks. The V2G systems provide electric energy to Electric automobiles (EAMs) to charge their batteries through aggregating charge stations (ACSs) upon which EAMs are able to function and run.

While EAMs are fast replacing conventional Internal Combustion Engines (ICEs), there are emerging threats in terms of security and efficiency in this domain. Since the sensors and devices in V2G frameworks are often resource constraint as no complex hardware is deployed, mutual authentication among different entities involved in V2G systems, confidentiality and privacy preservation of personal data remains a challenging task. This research proposed a novel user key exchange authentication scheme (NUKA) for V2G based frameworks addressing mutual authentication, data confidentiality and integrity as well as privacy preservation of all involved entities. Informal and formal analysis of NUKA in terms of efficiency and security showed that the proposed scheme is lightweight with enhanced performance and maximum security features as compared to existing schemes.

6.2 Summary of Research Contributions

The research in this thesis set forth our motivation and gave an overview of V2G networks. Chapter 2 discussed existing schemes for V2G systems, their merits and demerits, and drew a comprehensive analysis of their security and performance features which led us to the vulnerabilities of different types and need for a novel user key exchange authentication scheme for V2G based frameworks. which was presented in Chapter 3 with well defined threat model and security goals. Chapter 4 discussed formal security analysis of the proposed authentication scheme carried out by Proverif as well as BAN Logic and showed that the security goals defined in Chapter 3 are achieved successfully. Chapter 5 presented the performance analysis of proposed scheme with respect to computation and execution time. It also put forward a comparison analysis of different security features with existing state-of-the-art V2G protocols.

6.3 Conclusion

In this thesis, we have put forward a novel user key exchange authentication scheme for V2G based frameworks. We proposed a V2G network with three major entities: EAM, ACS, and GS and defined an adversary with certain capabilities. Our protocol uses PUFs and offers mutual authentication among all legitimate entities. Every session is carried out under pseudo-identities of EAMs and ACSs and 2 shared session keys (between EAM & GS and between ACS & GS) that are generated at grid station server and updated for every session. We showed the NUKA provides the security attributes of MA, identity protection, scalability, forward / backward secrecy, session key protection, physical security, message confidentiality and integrity. It is also resistant against MITM, replay, impersonation, DOS attack and traceability risks. NUKA is formally proven by Proverif and BAN Logic. In terms of operational capacity and computational efficiency, our approach outperforms the other schemes. Hence, NUKA is a feasible solution for threats being faced by V2G systems based networks.

6.4 Future Works

Our research was directed towards mutual authentication among different legitimate entities of V2G systems based networks. While we have achieved our defined security goals, there are still some challenges that need to be addressed, some of which are discussed as follows:

6.4.1 Rogue Charge Station

In case of physical capture of charging station, we have already established that no crucial data is stored on device memory. However, it can either be dismounted or the adversary can try to get it registered to any other grid station or some other commercial electric power supply provider. Posing as a legit charge station, it can cause power as well as economical damage to the system. There is no way of verification in this scenario and is an open source for future study.

6.4.2 Cyber Physical Attacks

Since the sensors and devices used in V2G systems are generally small, inexpensive and resource constraint, an adversary can launch multiple attacks on smart grids as most of their data *e.g.* transaction history, payment schedules, billing information etc. are usually outsourced for storage and along with this data, crucial information like private credentials of EAMs and ACSs are also transmitted over a public channel making cyber physical attacks a major challenge.

6.4.3 Electric Automobile Theft

All the electric automobiles are registered with the grid station. In case a theft of EAM occurs, there is no mechanism to verify the EAM owner. All the transactions are done with respect to EAM's identity so an adversary can steal a car and use it for any kind of malicious and / or criminal activity. It may also leak / sell the EAM owner's personal credentials without their consent to third-party where this information can be used in illegal activities. Hence, a need to authenticate the EAM owner or to provide GS with capability to detect such an activity and drop the specific EAM from registration terminating all future sessions; is a challenging future study.

6.4.4 Electric Automobiles' Maintenance Issues

Electric automobiles run on their electric batteries which require constant maintenance and replacement after a specific time period. This installation / un-installation of electric batteries are done in special centres with technicians with ample knowledge of EAM workings. This provides EAM access to a lot of people who are untrusted and can try foul play with EAM credentials. An adversary can exploit the EAM system by installing a chip like equipment or trapdoor to monitor power transactions and launch passive attacks. Detective and preventive measures to ensure security and privacy of EAM credentials in this scenario is an open source for future research.

References

[1] Benjamin K Sovacool and Richard F Hirsh. Beyond batteries: An examination of the benefits and barriers to plug-in hybrid electric vehicles (phevs) and a vehicle-to-grid (v2g) transition. Energy Policy, 37(3):1095–1103, 2009.

[2] Corey D White and K Max Zhang. Using vehicle-to-grid technology for frequency regulation and peak-load reduction. Journal of Power Sources, 196 (8):3972–3980, 2011.

[3] MD Shahrukh Adnan Khan, Kazi Mahtab Kadir, Khandaker Sultan Mahmood, Md Ibrahim Ibne Alam, Ainun Kamal, and Md Mamoon Al Bashir. Technical investigation on v2g, s2v, and v2i for next generation smart city planning. Journal of Electronic Science and Technology, 17(4):100010, 2019.

[4] Huaqun Wang, Bo Qin, Qianhong Wu, Li Xu, and Josep Domingo-Ferrer. Tpp: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids. IEEE Transactions on Information Forensics and Security, 10(11):2340–2351, 2015.

[5] Girraj Kumar Verma, BB Singh, Neeraj Kumar, and Vinay Chamola. Cbcas: Certificate-based efficient signature scheme with compact aggregation for

industrial internet of things environment. IEEE Internet of Things Journal, 7(4):2563–2572, 2019.

[6] Asmaa Abdallah and Xuemin Shen. Lightweight security and privacy-preserving scheme for v2g connection. In 2015 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE, 2015.

[7] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: application areas, security threats, and solution architectures. IEEE Access, 7:82721–82743, 2019.

[8] Muhammad Shahbaz, Changyuan Gao, LiLi Zhai, Fakhar Shahzad, and Imran Khan. Environmental air pollution management system: Predicting user adoption behavior of big data analytics. Technology in Society, 64:101473, 2021.

[9] Hui Liu, Zechun Hu, Yonghua Song, and Jin Lin. Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands. IEEE Transactions on Power Systems, 28(3):3480–3489, 2013.

[10] Henrik Lund and Willett Kempton. Integration of renewable energy into the transport and electricity sectors through v2g. Energy policy, 36(9):3578–3587, 2008.

[11] Najeeb Ullah. Electric vehicles in pakistan: Policy recommendations volume i cars. Energy Inst., Lahore Univ. Manage. Sci., Lahore, Pakistan, Tech. Rep, 2019.

[12] Qingqing Chen, György Csaba, Paolo Lugli, Ulf Schlichtmann, and Ulrich Rührmair. The bistable ring puf: A new architecture for strong physical unclonable functions. In 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, pages 134–141. IEEE, 2011.

[13] Roel Maes. Physically unclonable functions: Concept and constructions. In Physically Unclonable Functions, pages 11–48. Springer, 2013.

[14] Muhammad Naveed Aman, Kee Chaing Chua, and Biplab Sikdar. Mutual authentication in iot systems using physical unclonable functions. IEEE Internet of Things Journal, 4(5):1327–1340, 2017.

[15] Mahshid Delavar, Sattar Mirzakuchaki, and Javad Mohajeri. A ring oscillator-based puf with enhanced challenge-response pairs. Canadian Journal of Electrical and Computer Engineering, 39(2):174–180, 2016.

[16] Masoud Kaveh, Saeed Aghapour, Diego Martin, and Mohammad Reza Mosavi. A secure lightweight signcryption scheme for smart grid communications using reliable physically unclonable function. In 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), pages 1–6. IEEE, 2020.

[17] Prosanta Gope and Biplab Sikdar. Lightweight and privacy-preserving two-factor authentication scheme for iot devices. IEEE Internet of Things Journal, 6(1):580–589, 2019. doi: 10.1109/JIOT.2018.2846299.

[18] Yansong Gao, Yang Su, Lei Xu, and Damith C. Ranasinghe. Lightweight (reverse) fuzzy extractor with multiple reference puf responses. IEEE Transactions on Information Forensics and Security, 14(7):1887–1901, 2019. doi: 10.1109/TIFS.2018.2886624.

[19] Kai-Hsin Chuang, Erik Bury, Robin Degraeve, Ben Kaczer, Dimitri Linten, and Ingrid Verbauwhede. A physically unclonable function using soft oxide breakdown featuring 0% native ber and 51.8 fj/bit in 40-nm cmos. IEEE Journal of Solid-State Circuits, 54(10):2765–2776, 2019.

[20] Xuyang Lu, Lingyu Hong, and Kaushik Sengupta. Cmos optical pufs using noise-immune process-sensitive photonic crystals incorporating passive variations for robustness. IEEE Journal of Solid-State Circuits, 53(9):2709–2721, 2018.

[21] Wei-Che Wang, Yair Yona, Suhas N Diggavi, and Puneet Gupta. Design and analysis of stability-guaranteed pufs. IEEE Transactions on Information Forensics and Security, 13(4):978–992, 2017.

[22] Sujay Pandey, Sabyasachi Deyati, Adit Singh, and Abhijit Chatterjee. Noise-resilient sram physically unclonable function design for security. In 2016 IEEE 25th Asian Test Symposium (ATS), pages 55–60. IEEE, 2016.

[23] Duhyun Jeon, Jong Hak Baek, Dong Kyue Kim, and Byong-Deok Choi. Towards zero bit-error-rate physical unclonable function: Mismatch-based vs. physical-based approaches in standard cmos technology. In 2015 Euromicro Conference on Digital System Design, pages 407–414. IEEE, 2015.

[24] Ahmed Raheeq Sultan, Imran Rashid, Fawad Khan, Shahzaib Tahir, Maruf Pasha, and Aiman Sultan. A new secure authentication based distance bounding protocol. PeerJ Computer Science, 7:e517, 2021.

[25] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. 1999.

[26] Abdullah Al Hasib and Abul Ahsan Md Mahmudul Haque. A comparative study of the performance and security issues of aes and rsa cryptography. In 2008 Third International Conference on Convergence and Hybrid Information Technology, volume 2, pages 505–510. IEEE, 2008.

[27] Uwakwe C Chukwu and Satish M Mahajan. Modeling of v2g net energy injection into the grid. In 2017 6th International Conference on Clean Electrical Power (ICCEP), pages 437–440. IEEE, 2017.

[28] Sekyung Han, Soohee Han, and Kaoru Sezaki. Development of an optimal vehicle-to-grid aggregator for frequency regulation. IEEE Transactions on smart grid, 1(1):65–72, 2010.

[29] Fabian Kennel, Daniel Görges, and Steven Liu. Energy management for smart grids with electric vehicles based on hierarchical mpc. IEEE Transactions on industrial informatics, 9(3):1528–1537, 2012.

[30] Christophe Guille and George Gross. A conceptual framework for the vehicle-to-grid (v2g) implementation. Energy policy, 37(11):4379–4390, 2009.

[31] Benjamin K Sovacool and Richard F Hirsh. Beyond batteries: An examina-

tion of the benefits and barriers to plug-in hybrid electric vehicles (phevs) and a vehicle-to-grid (v2g) transition. Energy Policy, 37(3):1095–1103, 2009.

[32] Luis Pieltain Fernandez, Tomás Gómez San Román, Rafael Cossent, Carlos Mateo Domingo, and Pablo Frias. Assessment of the impact of plug-in electric vehicles on distribution networks. IEEE transactions on power systems, 26(1):206–213, 2010.

[33] Neetesh Saxena, Santiago Grijalva, Victor Chukwuka, and Athanasios V Vasilakos. Network security and privacy challenges in smart vehicle-to-grid. IEEE Wireless Communications, 24(4):88–98, 2017.

[34] Zhenyu Yang, Shucheng Yu, Wenjing Lou, and Cong Liu. pΘ{2}: Privacy-preserving communication and precise reward architecture for v2g networks in smart grid. IEEE Transactions on Smart Grid, 2(4):697–706, 2011.

[35] Xiaofeng Chen, Fangguo Zhang, and Shengli Liu. Id-based restrictive partially blind signatures and applications. Journal of Systems and Software, 80(2): 164–171, 2007.

[36] Hong Liu, Huansheng Ning, Yan Zhang, and Laurence T Yang. Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid. IEEE Transactions on Smart Grid, 3(4):1722–1733, 2012.

[37] Hong Liu, Huansheng Ning, Yan Zhang, Qingxu Xiong, and Laurence T Yang. Role-dependent privacy preservation for secure v2g networks in the smart grid. IEEE Transactions on Information Forensics and Security, 9(2): 208–220, 2013.

[38] Jia-Lun Tsai and Nai-Wei Lo. Secure anonymous key distribution scheme for smart grid. IEEE transactions on smart grid, 7(2):906–914, 2015.

[39] Ryuichi Sakai, Masao Kasahara, et al. Id based cryptosystems with pairing on elliptic curve. IACR Cryptol. ePrint Arch., 2003:54, 2003.

[40] Paulo SLM Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In International conference on the theory and application of cryptology and information security, pages 515–532. Springer, 2005.

[41] Vanga Odelu, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti. Provably secure authenticated key agreement scheme for smart grid. IEEE Transactions on Smart Grid, 9(3):1900–1910, 2016.

[42] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In International conference on the theory and applications of cryptographic techniques, pages 453–474. Springer, 2001.

[43] Asmaa Abdallah and Xuemin Sherman Shen. Lightweight authentication and privacy-preserving scheme for v2g connections. IEEE Transactions on Vehicular Technology, 66(3):2615–2629, 2016.

[44] Markku-Juhani O Saarinen. The bluejay ultra-lightweight hybrid cryptosystem. In 2012 IEEE Symposium on Security and Privacy Workshops, pages 27–32. IEEE, 2012.

[45] Honorio Martín, Enrique San Millán, Luis Entrena, Julio César Hernández Castro, and Pedro Peris López. Akari-x: A pseudorandom number generator for secure lightweight systems. In 2011 IEEE 17th International On-Line Testing Symposium, pages 228–233. IEEE, 2011.

[46] Jian Shen, Tianqi Zhou, Fushan Wei, Xingming Sun, and Yang Xiang. Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things. IEEE Internet of things Journal, 5(4):2526–2536, 2017.

[47] Huaqun Guo, Yongdong Wu, Feng Bao, Hongmei Chen, and Maode Ma. Ubapv2g: A unique batch authentication protocol for vehicle-to-grid communications. IEEE Transactions on Smart Grid, 2(4):707–714, 2011.

[48] Hong Liu, Huansheng Ning, Yan Zhang, and Mohsen Guizani. Battery status-aware authentication scheme for v2g networks in smart grid. IEEE Transactions on Smart Grid, 4(1):99–110, 2013.

[49] Jie Chen, Yueyu Zhang, and Wencong Su. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-grid (v2g) networks. China Communications, 12(3):9–19, 2015.

[50] Neetesh Saxena and Bong Jun Choi. Authentication scheme for flexible charging and discharging of mobile vehicles in the v2g networks. IEEE Transactions on Information Forensics and Security, 11(7):1438–1452, 2016.

[51] Prosanta Gope and Biplab Sikdar. Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart

grids. IEEE Transactions on Information Forensics and Security, 14(6):1554–1566, 2018.

[52] Prosanta Gope and Biplab Sikdar. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. IEEE Transactions on Smart Grid, 10(6):6607–6618, 2019.

[53] Mostafa M Fouda, Zubair Md Fadlullah, Nei Kato, Rongxing Lu, and Xuemin Sherman Shen. A lightweight message authentication scheme for smart grid communications. IEEE Transactions on Smart grid, 2(4):675–685, 2011.

[54] Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4):1015–1028, 2015.

[55] Ming Tao, Kaoru Ota, Mianxiong Dong, and Zhuzhong Qian. Accessauth: Capacity-aware security access authentication in federated-iot-enabled v2g networks. Journal of Parallel and Distributed Computing, 118:107–117, 2018.

[56] Yixin Su, Gang Shen, and Mingwu Zhang. A novel privacy-preserving authentication scheme for v2g networks. IEEE Systems Journal, 14(2):1963–1971, 2019.

[57] Dariush Abbasinezhad-Mood, Arezou Ostad-Sharif, Sayyed Majid Mazinani, and Morteza Nikooghadam. Provably secure escrow-less chebyshev chaotic

map-based key agreement protocol for vehicle to grid connections with privacy protection. IEEE Transactions on Industrial Informatics, 16(12):7287–7294, 2020.

[58] Gaurang Bansal, Naren Naren, Vinay Chamola, Biplab Sikdar, Neeraj Kumar, and Mohsen Guizani. Lightweight mutual authentication protocol for v2g using physical unclonable function. IEEE Transactions on Vehicular Technology, 69(7):7234–7246, 2020.

[59] Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. Design and implementation of puf-based" unclonable" rfid ics for anti-counterfeiting and security applications. In 2008 IEEE international conference on RFID, pages 58–64. IEEE, 2008.

[60] Wenbo Mao and Colin Boyd. Towards formal analysis of security protocols. In [1993] Proceedings Computer Security Foundations Workshop VI, pages 147–158. IEEE, 1993.

[61] Masoud Kaveh, Diego Martín, and Mohammad Reza Mosavi. A lightweight authentication scheme for v2g communications: A puf-based approach ensuring cyber/physical security and identity/location privacy. Electronics, 9(9): 1479, 2020.

[62] Bruno Blanchet et al. An efficient cryptographic protocol verifier based on prolog rules. In csfw, volume 1, pages 82–96, 2001.

[63] Alessandra Lumini and Loris Nanni. An improved biohashing for human authentication. Pattern recognition, 40(3):1057–1065, 2007.

[64] Timo Kyntaja. A logic of authentication by burrows, abadi and needham. Science Helsinki University of Technology, Tehran. http://www. tml. tkk. fi/Opinnot/Tik-110.501/1995/ban. html, 1995.

[65] Khwaja Mansoor, Anwar Ghani, Shehzad Ashraf Chaudhry, Shahaboddin Shamshirband, Shahbaz Ahmed Khan Ghayyur, and Amir Mosavi. Securing iot-based rfid systems: A robust authentication protocol using symmetric cryptography. Sensors, 19(21):4752, 2019.

[66] Soubhagya Sutar, Arnab Raha, and Vijay Raghunathan. Memory-based combination pufs for device authentication in embedded systems. IEEE Transactions on Multi-Scale Computing Systems, 4(4):793–810, 2018.

[67] Prosanta Gope, Jemin Lee, and Tony QS Quek. Lightweight and practical anonymous authentication protocol for rfid systems using physically unclonable functions. IEEE Transactions on Information Forensics and Security, 13 (11):2831–2843, 2018.

[68] H Hakan Kilinc and Tugrul Yanik. A survey of sip authentication and key agreement schemes. IEEE Communications Surveys & Tutorials, 16(2):1005–1023, 2013.

[69] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical unclonable functions and applications: A tutorial. Proceedings of the IEEE, 102(8):1126–1141, 2014.