CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

A Comparative Analysis Based Survey of Authentication and Encryption Schemes Used in VANETs

by

Muhammad Majid Zaman

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2020

I dedicate my work to My Family, My Teachers and Friends. A very special thanks to my Father, Mother, Wife and Brothers who always supported me. Also a very special thanks to my supervisor who motivated me and gave me confidence which enabled me to reach this goal.

CERTIFICATE OF APPROVAL

A Comparative Analysis Based Survey of Authentication and Encryption Schemes used in VANETs

by

Muhammad Majid Zaman

(MCS173064)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Muhammad Arshad Islam	FAST NUCES, Islamabad
(b)	Internal Examiner	Dr. Aamir Qayyum	CUST, Islamabad
(c)	Supervisor	Dr. Qamar Mehmood	CUST, Islamabad

Dr. Qamar Mehmood
Thesis Supervisor
July, 2020

Dr. Nayyer Masood
Head
Dept. of Computer Science
July, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
July, 2020

Author's Declaration

I, **Muhammad Majid Zaman** hereby state that my MS thesis titled "**A Comparative Analysis Based Survey of Authentication and Encryption Schemes Used in VANETs**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Muhammad Majid Zaman)
Registration No:MCS173064

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Comparative Analysis Based Survey of Authentication and Encryption Schemes Used in VANETs**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Muhammad Majid Zaman)
Registration No:MCS173064

Acknowledgements

"Recite in the name of your Lord who created. Created man from a clinging substance. Recite, and your Lord is the most Generous. Who taught by the pen. Taught man that which he knew not". Al-Quran[96:1-5]. I would like thank ALLAH Almighty for the will and determination to complete this work.

I am thankful to My Parents for their prayers, support and encouragement which kept me motivated through hot and cold, in ups and downs of my education and kept me going. so, I reached this milestone. Thanks to my Brothers they saw what no one saw and pushed my forward and thanks to my Wife, who did her best so that i could make the last miles towards my goal. I would also like to thank my friends who believed in me and supported me through out my life.

A special thanks to my supervisor **Dr. Qamar Mehmood** for his support and guidance. Thank you Sir.

(Muhammad Majid Zaman)

Registration No:MCS173064

Abstract

The idea of autonomous or self-driving vehicles is becoming a reality. And this all made possible due to vehicular ad-hoc networks (VANETs). VANETs was proposed to improve driving conditions as well as travelers safety, and this all is achieved by mutual exchange of messages among vehicles and infrastructure. The access to the network is open which makes information security and privacy a major concern. An attacker can capture, modify, replay or delete the messages which can cause traffic jams or even roadside accidents. No structured comparative analysis of authentication and encryption schemes for VANETs is available. The existing surveys for VANETs are not structured and are not based on taxonomies. In this thesis, we will analyze the authentication and encryption schemes for VANETs in a structured way. we will construct the taxonomies of respective schemes and identify research gaps using the taxonomies. Finally, we will highlight authentication and encryption schemes that could be used to provide desired security with low computational cost.

Contents

List of Figures

List of Tables

Abbreviations

BS	Base Station
CA	Certification Authority
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
IBC	ID Based Cryptography
LWC	Light Weight Cryptography
OBU	On-Board Unit
PKG	Private Key Generator
PKI	Public Key Infrastructure
RSU	Road Side Unit
TESLA	Time-Efficient Stream Loss-tolerant Authentication
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure

Chapter 1

Introduction

1.1 Background

People around the globe use their private vehicles every day for getting to their destinations. Growing population and economic stability enabled one to own more than one vehicles. Road traffic jams and accidents are a common sight now a day. VANET (Vehicular Ad-hoc Network) was proposed to keep traveler safe and roads clear from congestion.

VANET is a subset of the mobile ad-hoc network (MANET) where routes (roads) are predefined. It depends on Roadside units (RSUs) and On-Board units (OBUs) for registration and management. RSUs are placed on the road junctions to fulfill specific services and OBUs are installed in the vehicles navigating in VANET. All vehicles are moving freely on road network and communicating with each other or with RSUs and specific authorities.

Although VANETs is a sub-type of MANETs. Here are some of the difference.

- MANETs have no central body (server or base station) [1]
- High mobility of nodes and time critical information is exchanged in VANETs[2].
- Frequent disconnections in VANETs[2].

- Scale of the network in VANET is much larger than that of MANETs[3] High application requirements, attacks like Sybil attack, black hole attack and timing attacks in VANETs[4]
- In VANETs, network density is variable. Network becomes dense in rush hours or traffic jams whereas it becomes less dense in night times[5].
- Restricted or strict mobility pattern of vehicles in VANET[6].
- MANETs suffer from scalability issues.

As MANETs and VANETs both are ad hoc networks. Due to the above mentioned differences security protocols used in MANETs cannot be used in VANETs without changes applied to them [4].
VANETs communication modes are V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure). These modes use DSRC (Dedicated Short-Range Communication) that is a type of communication which is designed for automobiles to communicate with other vehicles and infrastructure. DSRC uses band such as GSM, UMTS or WiMAX network[7].
In VANETs all communication is done through messages in the wireless medium. The wireless medium used in VANETs is not secure due to its open nature and high mobility environment. It has drawbacks which make the network vulnerable for different types of attacks (Sybil, DoS, Masquerading, Man-in-the-middle, wormhole attack). These attacks compromise integrity (man-in-the-middle, replay attack), confidentiality (Man-in-the-middle, wormhole), availability (DoS) and authentication (Sybil, node impersonating) of messages. An Attackers aim is to transmit manipulated or modified information from source to destination which causes road blocks, road accidents[7].

In VANETs, a number of attacks are performed, some of attacks are discussed here. Sybil attack involves an attacker using multiple identities at the time and broadcasts false messages[8]. In DoS (Denial of Service) attack, attacker blocks the communication and stops the services, so they are not available to the users.
In Masquerading attack, attacker uses a valid identity to produce false messages.

In Node impersonating attack, attacker attain a valid id and enters the network. In wormhole attack, attacker broadcasts a false message to legitimate users and non-neighbor nodes to exchange control packets. Man-in-the-middle attack involves an attacker inserts itself between two victims and controls their mutual communication[7].

In Replay attack, attacker captures the valid emergency messages and transmits them after sometime[9] Encryption is used for data protection to avoid unauthorized access. Whereas authentication is the process of verifying a user for its legitimacy. VANET uses a number of authentication schemes like multilevel, threshold anonymous, pairing free certificate less, privacy preserving, cooperative message, group signature, enhanced, light weight, scalable robust.

For encryption VANET uses standard encryption algorithms ID based cryptography, AES, ECDSA. Authentication in VANETs ensures that valid and trusted user or vehicle enters into the network. Encryption in VANETS ensures the messages being transmitted reaches its destination without any modification to its contents.

1.2 Terminologies about VANETs

In this section we will define some common terms used in VANETs. The definition of terms provide an easy understanding and provides an overview of the VANETs.

Road Side Unit (RSU): It is a communication entity which is deployed on the road or on the intersections for communication between vehicles and infrastructure [7]. **Vehicle-to-Infrastructure (V2I)**: it is the name given to the communication happening between vehicle and infrastructure or RSU [7].

Vehicle-to-Vehicle (V2V): It is the name given to the communication happening between vehicles [10].

On-Board Unit (OBU): it is the communication and tracking equipment installed in every vehicle for information sharing with RSUs and other vehicles [7].

DSRC (Dedicated Short Range Communication): It is a type of communication that is designed for automobiles to communicate with other vehicles and

infrastructure [7].

Certification Authority/ Trusted Authority (CA/TA): it is an entity that is used to register both RSUs and vehicles. It assigns certificates and a pair of keys to vehicles and RSUs. It also authenticates both RSUs and vehicles whenever requested[7].

Pseudonym: it is an identity provided to a vehicle by Certification Authority(CA), which is to be used by the vehicle instead of its real identity while communicating with other vehicles and communicating with RSU [11] .

Revocation List: It is the list of vehicles that are banned or revoked from communicating within the network due to malicious activity or involvement in a dispute [12].

PKI: it stands for Public Key Infrastructure. In PKI, a pair of a public and private key is used for encryption and decryption. For encryption, the public key of the receiver is used. While the private key of the decryption [10].

Public Key: It is the publically known parameter of a vehicle or node used to encrypt a message [2].

Private Key: It is the secret parameter known only to a vehicle or node which the key belongs to and is used to decrypt a message which was encrypted using it's (receivers) public key [2].

Group Key: It is the secret key known to all members of a communication group formed by an RSU. The messages within a group are encrypted and decrypted using a group key [13].

PKG: it stands for a Private key generator. It is the entity that generates the private key of a message receiver which is used to decrypt a received message [14].

IBC: it stands for Identity based cryptography. It is an encryption/cryptographic technique in which messages are encrypted using publically known parameter like phone number, email id or registration number of message receiver [14].

ECC: It stands for Elliptic curve cryptography. It is an encryption technique that is based on an algebraic curve over the finite field [2].

ECDSA: It stands for elliptic curve digital signature algorithm. It uses elliptic curve cryptography to generate digital signatures [15].

Digital Signature: It is a code attached to a message while sending it electronically for authenticating and verifying message contents and message sender. A digital signature is created using the private key of the sender and this can be verified by using the public key of message sender [16].

Certificate: A digital certificate is a digital document that consists of a vehicles unique identity, the validity of public and private keys. Certificates are used for encryption and authentication. It is issued by the Certification Authority(CA) [16].

LWC: It stands for Lightweight cryptography. It is an encryption or cryptographic technique that was proposed to be used as a replacement of conventional encryption algorithms in environments where memory and computational power is limited [17].

Mutual Authentication: It is an authentication approach in which both the entities message source and destination authenticate each other [18].

TESLA: It stands for Time-Efficient Stream Loss-tolerant Authentication. it is an authentication scheme used for communication, which uses symmetric encryption. It implements a broadcast authentication, which is the same as unicast authentication [17].

1.3 Motivation

Structured analysis of authentication and encryption schemes is not available. The currently surveys available for VANETs is not structured according to the taxonomies for domain of authentication and encryption schemes for VANETs.

1.4 Problem Statement

No comparative analysis of authentication and encryption schemes for VANETs. The existing surveys are not structured and not based on taxonomy.

1.5 Research Questions

On the basis of above described problem statement we have identified following research questions.

Research Question 1:

Is there any comparative study related to authentication and encryption schemes available in VANETs?

Research Question 2:

How comparative analysis will be performed in a structured way?

Research Questions 3:

How research gaps will be identified using the comparative analysis?

1.6 Research Methodology

Research methodology of our thesis is as follows

- Research articles related to authentication and encryption schemes were collected
- Comparative analysis was performed
- Tables and hierarchies were constructed

The detail research methodology will be explained in chapter 3.

1.7 Organization of the Thesis

The remainder of this thesis is organized as follows. In chapter 2, we will present the literature review. In chapter 3, we will introduce the research methodology and experiment. In chapter 4, we will present results and findings also explain our tables and hierarchies, and in chapter 5 we will conclude the thesis with future tasks.

Chapter 2

Literature Review

2.1 Introduction to Survey

In this chapter we will present literature review of authentication, encryption schemes used in VANETs and comparison of existing surveys. First we will discuss the authentication schemes followed by encryption schemes. Then, we will discuss and compare existing surveys with our work.

2.1.1 Authentication Schemes

In this section will review the authentication schemes used in VANETs
Adigun et.al[19] proposed Pseudonym change protocol. this technique consists of two approaches. In the first approach, vehicle always communicates to get its pseudonym from certification authority. In the second approach, vehicle updates its pseudonym and certificate once the vehicle is authenticated by Certification authority. This protocol uses both asymmetric and symmetric encryption techniques. Encryption is used for information protection. This protocol was tested in city environment and it bandwidth extensive.
Younes et.al[20] proposed a secure traffic congestion control protocol. In this technique, RSU registers itself to key distribution center (KDC) and certificate server

(CS). When a vehicle wants to communicate with RSU, first it authenticates the RSU with CS. When CS authenticates RSU, vehicle requests to join the network. RSU forms a group of vehicles travelling a specific road segment. Asymmetric encryption is used in this technique. Encryption is used for authentication. Hashed MAC is used for information protection.

Zeng et.al[18] proposed mix context based pseudonym changing privacy preserving authentication scheme This technique consists of three phases, initialization, registration and mutual authentication. In initialization phase, public and private keys for Trusted Authority (TA) are generated. In registration phase, both RSU and vehicle gets registered with TA. TA provides both RSU and vehicle with public and private keys also with temporary ids. When RSU vehicle communicates with other vehicle or RSU, it is authenticated by communication receiver itself and authentication process does not involve TA. Asymmetric encryption is used. Encryption is used for message protection while hash function is used for authentication.

Liu et.al[21] proposed lattice based anonymous authentication scheme. This scheme consists of four phases. In first phase, private and public keys for the system are generated. Second phase, private and public keys are assigned to vehicles and RSUs using their ids respectively. In third phase, RSUs and Vehicles generate their signatures. In forth phase, received messages are verified or authenticated using signature computation. This scheme uses asymmetric encryption. This scheme uses no Temper Proof Device (TPD).

Liu et.al[21] proposed a secure and efficient group key agreement scheme. symmetric encryption is used along with two secure hash functions. In this scheme, registration phase includes the exchange of vehicles and RSUs information to each of RSU and vehicle by trusted authority (TA). In second phase, RSU authenticates the vehicle to form group of vehicles. This group of vehicle uses group key for message exchange. Here encryption is used for authentication while hash function provides message integrity.

Wang et. al[22] proposed A Practical Authentication Framework which is based on conditional privacy preserving authentication (CPPA) scheme. In CPPA scheme,

true identity of the user or vehicle remains hidden until the user or vehicle is found to be involved in malicious activity or in a dispute. During this whole process, vehicle or user uses a temporary id called pseudonym. This scheme uses symmetric encryption. Encryption for information security while hash function for authentication purposes.

caballero-gil et. al[23] proposed mutual authentication scheme. this scheme uses asymmetric encryption. Three phases in this scheme. first is discovery, in which nodes discover each other and check for availability of their respective public keys. If keys exist, they simply use those key to authenticate each other. If no keys exist, second phase starts. Nodes store keys of each other is 3 graphs that are used for authentication and key store.

Desales et.al[8] proposed A Privacy-preserving Authentication and Sybil detection Protocol. asymmetric encryption is used in this scheme. four phases in this scheme, registration, temporary id, Sybil detection and prosecution. In first phase, vehicles are registered with Certification authority (CA). CA assigns public, private keys and temporary id. In second phase, vehicle requests RSU for temporary keys. In this phase, both vehicle and RSU authenticate each other. Third phase involves Sybil attack detection. In forth phase, malicious or Sybil node is prosecuted and its connection is terminated.

Lu et. al[24] proposed a block chain-based anonymous reputation system for trust management scheme. this scheme uses asymmetric encryption. This scheme involves tfour steps. In first step, vehicles are registered with certification authority (CA). CA assigns initial key pair and certificate. In second step, vehicle authenticates itself to get certificate update with CA before initial certificate expires. In third step, if vehicle is found to be malicious, its public key is revoked. Thus stopping any communication from malicious vehicle. Authentication process involves checking the vehicles keys in certification and revocation list.

Casola et.al[25] proposed an interoperability system for authentication and authorization. This scheme involves asynchronous communication between vehicles and between vehicle and infrastructure. In vehicle and infrastructure communication, vehicle requests for certificate. Server generates an id number and acknowledges

the request with this id. Using this id number server generates the certificate and sends certificate to vehicle after authenticating, authorizing and determines services required by the vehicle. In vehicle to vehicle communication, vehicle send the message to other vehicle using its certificate. Receiving vehicle requests server to evaluate the certificate of sender. Id number against the certificate is retrieved and certificate is evaluated. The results of authentication and authorizing process is forwarded to receiver vehicle.

Huang et. al [11] proposed an efficient pseudonymous authentication based conditional privacy protocol. this scheme uses symmetric encryption. This scheme has three blocks namely, registration, generation and extraction. In first block, the vehicle get itself registered by motor vehicle division (MVD). MVD assigns a ticket to the vehicle. This ticket is used by vehicle to generate its certificate and MVD uses this ticket to track the vehicle. In second block, vehicle presents its ticket to RSU. Using ticket provided by the vehicle, RSU generates the token and sends it to vehicle. In third block, vehicle uses this ticket to generate pseudonym. This pseudonym will be used instead of real id during communication.

Wang et. al[12] proposed lightweight and efficient strong privacy preserving authentication scheme. this scheme uses asymmetric encryption. This scheme consists of six phases namely registration, signing, verification, updating system keys, revocation and tracing. In registration phase, vehicles get registered with key management center (KMC). KMC generates public, private keys and other system parameters. KMC provides access token to the vehicle when registration process completes. In signing phase, vehicle generates a message and time stamps it. Before sending the message, vehicle signs it. Token stored in the temper proof device (TPD) is compared with the token sent by the TPD. If the two tokens match, message is signed and the message is sent. Message contains message data, mac code of the message, time stamp and pseudo-id of the sending vehicle. In verification phase, the access token is verified. Mac of message is computed and compared with received mac code. In system key update phase, the system keys are updated periodically. This is to avoid misusage of TPD. In revocation phase, if a vehicle is found in malicious activity, the vehicles delete its pseudo-id thus

making malicious vehicle unable to communicate. In message tracing phase, the messages are tracked by KMC.

varshney et. al[26] proposed security protocol for VANET by using digital certification to provide security with low bandwidth scheme. this scheme consists of three phases. In first phase, infrastructure components of the network, base station (BS) and road side unit (RSU) communicate with each other. The communication between BS and RSU is symmetric. BS provides certificate and public key to RSU. The symmetric encryption here used is for authentication. In second phase, Vehicle and RSU communicate with each other. The vehicle is registered with RSU. Vehicle and RSU share their certificates and ids with each other. This way mutual authentication is achieved. In third phase, vehicle to vehicle communication takes place. The vehicles exchange their certificates and mutually authenticate is achieved.

Rajput et. al[27] proposed a two level privacy preserving pseudonymous authentication protocol. in this scheme, asymmetric encryption is used. This scheme consists of six steps. In first step, system is initialized and system entities generate their keys. In second step, vehicles are registered with CA. vehicle sends its id, and public private keys to CA. CA store these values in a data base and provides pseudonym to the vehicle. In third phase, vehicle and RSU communicate with each other. Vehicle generates new pair of keys and sends them to RSU with its pseudonym. RSU verifies this message with CA. in forth phase, RSU generates a short time pseudonym and shares it with vehicle. This pseudonym is used for vehicle to vehicle communication. In fifth step, vehicle requests CA for pseudonym after its initial pseudonym expires. In sixth step, if a vehicle is found in malicious activities, CA revokes it certificate.

Bayrak et. al[16] proposed a secure and privacy protecting protocol. this scheme uses asymmetric encryption. This scheme consists of three mechanisms. This scheme consists of three phases. In first phase, vehicles are registered with certification authority (CA). CA assigns public, private keys and certificate to the vehicles. In second phase, Vehicles communicate with RSUs and with other vehicles. Message signed using private key is considered as authentic because encryption is

this case is used as an authentication function. In third phase, malicious nodes are identified and their keys are revoked. CA changes the pair of keys and sends them to all vehicles except for malicious vehicle.

Fan et. al[28] proposed strongly privacy preserving communication protocol. this scheme consists of six phases. In first phase, trusted authority (TA) selects system parameters and publishes those parameters. In second phase, RSUs and vehicles get registered with TA. TA assigns pair of keys and certificate to RSU and vehicles. These keys and certificate is used in signing messages. In third phase, messages are transmitted. Vehicle sends a request to RSU to broadcast a message. RSU authenticates the vehicle, after authentication vehicle broadcast the message. In forth phase, vehicles receive and authenticate the sender. Vehicle first checks for time stamp then RSU signature is verified and then message is accepted. On fifth phase, vehicle is traced in case of dispute. Real id of the vehicle is transmitted to all RSU. In sixth phase, the vehicle which is in dispute or involved in malicious activity is revoked from network.

Xiong et. al[29] proposed Efficient and multi-level privacy-preserving communication protocol. this scheme consists of four phases. In first phase, system is initiated. Member manager (MM) selects system parameters. Vehicles select pair of keys from pool of keys and two integers. Vehicle then send its id, public key and two integers to MM. MM keeps record of public key and id of the vehicle. In second phase, message is generated and transmitted. The vehicle generates its signature and attaches to the message and sends the message. In third phase, message is verified by the receiving vehicle. if message is verified successfully, the receiving vehicle updates its public key. In forth phase, the MM will resolve a dispute. MM will look for vehicle id and public key. On finding the desired vehicles id, MM transmits the revocation message to all RSUs and OBUs. In this scheme asymmetric encryption is used, and it is used for authentication purposes.

Shen et. al[30] proposed lightweight privacy preserving protocol using chameleon hashing for secure vehicular communications scheme. this scheme consists of three phases namely registration, mutual authentication and tracking phase. In registration phase, CA registers OBUs and RSUs. CA assigns certificates to both RSUs

and OBUs. CA stores information about RSUs and OBUs in data base. In mutual authentication phase, both RSU and OBU generate their new private key and they exchange their public keys with each other. Both RSU and OBU authenticate each other with CA. in CA tracking phase, dispute settlement is performed. The real id of the OBU is recovered from data base by CA. in this scheme elliptic curve encryption technique is used.

mishra et.al[15] proposed a secure and efficient message authentication scheme. this scheme uses ECDSA private and public key. The first step of this scheme is vehicle registration with TA. Vehicle selects public and private keys and registers this key pair with id to TA. TA assigns certificate to the vehicle. In RSU deployment phase, RSUs are registered, deployed. The public key of the RSU is distributed among all registered vehicles. RSU assigns temporary id to vehicles entering into their coverage area. This temporary id is used by the vehicle to send messages.

Wasef et. al[31] proposed expedite message authentication protocol. this scheme uses asymmetric encryption. The first phase in this scheme is system initialization, the TA generates public and private keys and their corresponding certificates. These keys and certificates are embedded in OBU. In second phase which is message signing, vehicle checks its revocation then signs the message and broadcasts the message. The message contains message data, pseudo-id, HMAC code, time stamp and revocation check value. In third phase which is message verification, message receiving OBU performs revocation check. If the revocation checks fail, the message is dropped otherwise it is accepted.

Rajput et. al[32] proposed hierarchical privacy preserving pseudonymous authentication protocol. this scheme uses Elliptic curve cryptography. This scheme consists of six phases namely system initialization, registration and primary pseudonym generation, re-acquiring primary pseudonym, secondary pseudonym generation, beacon broadcast and vehicle revocation. In first phase, system parameters are defined and these parameters are downloaded by all network entities. In second phase, vehicle shares its public, private keys along with real id with CA. CA saves these parameters with time stamp in data base, and informs the vehicle about the

expiration time and provides pseudonym to the vehicle. In third phase, vehicle re-acquires the primary pseudonym when pseudonym expires. In forth phase, vehicle generates another pair of public, private keys and share this key pair along with pseudonym and shares it with RSU for communication purposes. RSU authenticates pseudonym from CA. once the vehicle is authenticated, RSU generates secondary pseudonym and shares it with vehicle. In fifth phase, vehicle attaches secondary pseudonym with message and broadcast the message. Receiver of the message authenticates the attached pseudonym from RSU. In sixth phase, malicious nodes are revoked from communication in network.

Bayrak et. al[16] proposed a secure and privacy protecting protocol for VANET. This scheme consists of three phases namely, certificate management, secure and private communication and certificate revocation. In first phase, certification authority (CA) generates and assigns two pair of public, private keys and certificate to the vehicles. Out of these two pair of keys, one will be used for emergency messages and second will be used for safety messages. In second phase, the vehicles communicate with each other. Time stamped messages are exchanged along with signature of the message sender. In third phase, malicious vehicles certificate is revoked.

2.1.2 Encryption Schemes

In this section will review the encryption schemes used in VANETs.

Huang et. al[11] proposed an efficient pseudonymous authentication based conditional privacy protocol for VANETs. This technique is based on four phases. In the first phase, system parameters and a ticket is assigned to vehicles by the Motor Vehicle Department(MVD). In the second phase, vehicle uses obtained ticket from MVD to generate its pseudonym. Vehicle uses this ticket to obtain tokens from RSU. In third phase, vehicle communicate with other vehicles using its pseudonym. In forth phase, vehicle involved in malicious activities or involved in a dispute is revoked from the network.

Baldini et. al[14] proposed Identity-Based Security systems for VANETs. In this scheme, they proposed use of Identity based encryption. Both sender and receiver are registered with Private key generator(PKG). As the name suggests, PKG is responsible for generating private keys for registered entities. For message sending, sender combines the message with its hashed identity of receiver which is used as public key and encrypts it using publically known identifier of the receiver. On receiving the message, receiver asks PKG for senders private key. Receiver uses this private key to decrypt the message.

Yeun et. al[33] proposed efficient security implementation for emergency in VANETs. In this paper, authors proposed use of ID-Based cryptosystem. This scheme consists of three main phases. In first phase, the encryption algorithm is selected. Setup of Private key generator(PKG) is performed. Keys are generated. In second phase, vehicles are registered and are authenticated. In this phase, message communication takes place. The messages are encrypted and signed before sending. On the receiver side, signatures are verified and decrypted to retrieve the message. In this phase, user registration is checked whether user is a member of the network or not.

Khan et. al[34] proposed secure multimedia delivery in vehicles using road side infrastructure. The proposed idea is an android application in which users are registered against vehicle registration number(VIN). The registered user generates the message, which encrypted using AES encryption algorithm. Secure Hash Algorithm (SHA-256) is used to generate hash of the encrypted message. Ad-hoc On-demand multipath distance vector routing (AOMDV) determines the route and sends the message. The message is divided into two portions, one portion goes to receiver and the other part goes to server which is used to register the user. The receiver, on receiving the message sends the message and its position to server which provides the receiver with the part of message which server received. The receiver combines both parts and calculates the hash of the message. If both hash values are same then message is decrypted.

Wang et. al[35] proposed anonymous data access scheme using pseudonym based cryptography. In this scheme, vehicles and RSUs are identified by their pseudonym

instead of real identity. In this scheme, the node generates route request and broadcast it. The receiving node checks for the validity of time stamp, if the time stamp is valid then, it keeps the source nodes information in routing table and reply the route request. The data request phase, a node generates the data request and sends it. The receiving node first checks for validity of the message. If the message is valid then it decrypts the message using session key.

Yan et. al 36 proposed location security in VANETs. In this scheme, the network cell to verify the location of other nodes. This scheme uses a geographical location-based security system. Messages are encrypted using geographical location key. The sender specifies the message decryption zone. To decrypt the message, the receiving vehicle must be present at the geographical decryption zone.

Burmester et. al [37] proposed strengthening privacy protection. In this scheme whenever a new node is discovered, discovering the vehicle sends an encrypted certificate encrypted using the new nodes public key. After authentication, nodes exchange a shared key which starts the process of mutual authentication.

Cho et. al[38] proposed an improved privacy preserving navigation protocol. this scheme consists of three phases namely, system setup, navigation credential request and navigation service request. In first phase, system parameters like secret keys, hash function are selected. Vehicles and RSU are registered and pair of public and private keys are provided. In order to navigate on the road securely the vehicle requests navigation credentials from RSU in second phase. Vehicle sends the request for credentials and RSU authenticates it. If the vehicle is authenticated successfully, RSU provides the vehicle with navigation credentials. In third phase, vehicle requests RSU for services for route guides towards its destination. Vehicles sends request with destination information to RSU. RSU first verifies the request then starts to search best route to the required destination. After discovering the route, RSU provides the requesting vehicle the discovered route.

Zhou et. al[39] proposed practical V2I secure communication schemes for heterogeneous VANETs. They proposed four techniques. In first technique, RSU uses ID-based cryptography(IBC) to receive messages from vehicles that are in public key infrastructure(PKI). In second technique, RSU uses PKI to broadcast cipher

text to vehicles that are in IBC. In third scheme, RSU uses IBC to send messages to vehicles in PKI. In forth phase, vehicles use IBC to send message to RSU in PKI.

Malik et. al [40] proposed an Asymmetric encryption-based secure and efficient data gathering technique in VANETs. At first, the vehicle and RSU make a secure connection. when the connection is established, the vehicle sends its information to RSU. RSU authenticates the received information by using CA. After the vehicle is verified successfully, RSU and vehicle start to communicate with each other. Messages are encrypted using the receivers public key. The receiver uses its private key to decrypt the encrypted message. RSU maintains a data table which is used to store data of verified vehicles, this table is used whenever a new message is received. RSU checks the table for vehicle identity. If the vehicles identity exists in the table, RSU attaches the identity information of the vehicle with the message. Otherwise, authentication is performed.

Zhu et. al [41] proposed SMSS: Symmetric-Masquerade Security Scheme for VANETs. This scheme consists of three phases. In the first phase, when a vehicle enters Base Station (BS), the BS assigns a pseudonym to the vehicle. In the second phase, BS assists the exchange of symmetric keys between two vehicles. In the third phase, vehicles communicate with each other. In case of an accident, vehicles can identify other vehicles by symmetric key they exchanged in the second phase without help from BS.

Anitha et. al [42] proposed Data security in VANET Dissemination using advanced cryptographic techniques. They proposed three techniques for data dissemination. In the first technique, they categorized the messages into emergency, entertainment, and general messages. The categorization of the messages is done through the use of keywords. In the second technique, a signcryption technique is used to protect the message from a midflight modification. This signcryption uses the AES algorithm which is based on the cuckoo search algorithm and Blowfish algorithm. In the third technique, they explained the optimal blowfish algorithm working.

Mutiri et. al 43 proposed Improving Vehicular Authentication in VANET using

Cryptography. They proposed using four-step authentication which uses a combination of techniques for confidential and three-step authentication for safety or emergency messages and these messages are not encrypted. In the four-step authentication process, the first step is named as challenge and response. In this step, for message exchange receiver asks the sender for his location information. The decision of whether to accept or reject the message is based on round trip time(RTT). In the second step, messages are signed using digital signatures. The private key is used for encryption which ensures messages are unaltered. In the third step, messages are time-stamped to confirm the keys of the message sender are not revoked. In the fourth step, the message is encrypted by using the private key of the receiver. Which ensures messages will reach and decrypted by the actual receiver. Roy et. al [44] proposed A Modified RSA Cryptography Algorithm for Security Enhancement in Vehicular Ad Hoc Networks. They compared the RSA algorithm with modified RSA (MRSA) algorithm by using the same size key and same size of data. They found that by increasing one prime number in MRSA and with the same key size MRSA outperforms RSA in terms of encryption and decryption time as well as in terms of security.

2.1.3 Exisiting VANETs Surveys

In this section will review the existing surveys in VANETs.

Biswas et. al[45] conducted a survey on security and privacy based on cryptography. They used privacy and anonymity approaches used in VANETs as parameters for their survey. They compared existing privacy techniques and highlighted their advantages and limitations. On the basis of their survey, they concluded that Tradeoff between security and privacy exists. For security, there is a compromise on privacy.

Haseeb et. al[46] conducted survey on authentication. They used authentication schemes as a parameter for their research. They conducted research to identify limitations and issues in authentication and digital signatures. They concluded

that authentication schemes should be made more efficient and require less computing power.

Bariah et. al[47] conducted survey on VANET security. They considered threats and security services proposed for those attacks for their research. They provided overview of treats and security services. They concluded that many aspects of security remained unexplored.

Dahiya et. al[48] surveyed user authentication schemes. They reviewed existing protocols. They concluded that user position could be used in authentication process.

Engoulou et. al[49] surveyed VANETs security. They discussed threats in VANETs, security requirements and security solutions. This survey provides overview of threats, attacks and attackers.

Gillani et. al[10] surveyed VANETs security. They discussed attacks, security challenges and security requirements. They reviewed existing security solutions and categorized those solutions. They reviewed all solutions in detail and identify that there exists no solution which resolves all known security issues.

Mejri et. al[7] surveyed VANET security and communication architecture on basis of cryptography. They reviewed attacks and cryptographic schemes in VANETs in detail. They compared all cryptographic schemes used in VANETs and analyzed security problems on the basis of cryptographic schemes.

Mejri et. al[50] reviewed cryptographic solutions for VANETs security. They reviewed attacks and security solutions in detail also provided an overview of proposed cryptographic solutions.

Moharrum et. al[51] discussed VANET security. They reviewed attacks in VANETs and solutions to attacks. On the basis of their review, they suggested that cell phone stations should be used to make VANETs communication cost effective.

Mishra et. al[52] reviewed VANETs security. They discussed attacks in VANETs and solutions to those attacks. They presented an overview of security solutions to attacks. They pointed out security as a major concern in VANETs.

Qu et. al[53] discussed security and privacy in VANETs. They performed a detail review of security, privacy issues and solutions to these issues. They identified

tradeoff between security and privacy.

Riley et. al[54] surveyed authentication schemes. They reviewed existing authentication schemes and performed comparison of these schemes. They identified that authentication is a research rich area of VANETs.

Sahare et. al[55] reviewed security and privacy approaches. They reviewed cryptographic techniques used in VANETs. Their research provided a wide analysis of threats and challenges in VANETs security.

Shaikh et. al[56] reviewed VANETs security. They reviewed cryptographic schemes used in VANETs. They compared RSA and ECC algorithms. The main focus of their research was strengths and limitations of RSA and ECC algorithms. They identified cases where these algorithms outperform each other.

Jashnani et. al[**?**] surveyed cryptographic techniques used in VANETs. They reviewed existing cryptographic techniques in order to identify a technique which provides desired privacy and security. They concluded that ECC is faster in encryption and RSA is faster in decryption.

Ali et. al[57] surveyed authentication and privacy schemes used in VANETs. They identified advantages and limitations of these schemes. They also identified issues like tradeoff between safety and privacy.

Sheikh et. al[58] surveyed VANETs security services. They reviewed attacks performed in VANETs, countermeasures to stop those attacks and authentication schemes. They identified security challenges and indicated possible solutions.

2.2 Conclusion

In this section we will conclude the existing survey review by comparing our work with existing surveys.

All of the above surveys are detail surveys and reviewed all VANETs security issues. First, however, our work is different from the above surveys in terms of classification of authentication and encryption schemes. For example, Biswas et. al [45] surveyed security of VANETs based on cryptographic schemes in terms of privacy and anonymity approaches. Haseeb et. al[46] surveyed authentication schemes in

terms of authentication methods. Bariah et.al[47] surveyed VANETs security in terms of security services and threats to VANETs. Dahiya et. al[48] surveyed user authentication in terms of authentication protocols used in VANETs. Engoulou et. al[49] surveyed VANETs security in terms of security threats, security requirement and security solutions. Gillani et. al[10] surveyed VANETs security in terms of attacks, security challenges and requirements. Mejri et. al[7] surveyed VANETs security and communication architecture on the basis of cryptographic techniques. They performed their review on the basis of attacks and cryptographic techniques used in VANETs. Mejri et. al[50] surveyed cryptographic solutions to VANETs security issues in terms of cryptographic schemes and security challenges. Mishra et. al[50] surveyed VANETs security in terms of attacks and security solutions. Moharrum et. al[51] surveyed VANETs security in terms of attacks and security solutions. They discussed the existing techniques ability to provide security. Qu et. al[53] surveyed VANETs security and privacy in terms of security issues, solutions to those issues and privacy solutions. Riley et. al[54] surveyed authentication schemes. They provided an overview of authentication schemes and performed a comparison between schemes. Sahare et. al[55] surveyed security approaches in terms of cryptographic techniques. Shaikh et. al[56] surveyed VANETs security in terms of cryptographic algorithms. They performed comparison of RSA and ECC cryptographic algorithms. Jashnani et. al[**?**] surveyed cryptographic techniques used in VANETs. They performed comparison of cryptographic algorithms. Ali et. al[57]surveyed authentication and privacy techniques used in VANETs. They identified strengths and limitations of these techniques. Sheikh et. al[58] surveyed VANETs security services in terms of attacks, countermeasures and authentication schemes. Secondly, we are considering two security mechanisms authentication and encryption while above mentioned surveys either consider authentication or encryption schemes for their research. We classified these schemes and composed their hierarchies respectively while, above mentioned surveys lacked hierarchies of these schemes.

Thirdly, we did not considered privacy or security issues and attacks on VANETs for our research which also makes our work different from existing.

In short, we considered authentication and encryption schemes used in VANETs without discussing security issues and attacks on VANETs and presented tabular layout, also presented hierarchies for the respective schemes to help identify research gaps in one document. While the existing surveys lacked both the tabular layout as well as hierarchies of authentication and encryption schemes.

Chapter 3

Research Methodology and Experiment

3.1 Introduction

In this chapter, we will explain our research methodology followed by the explanation of our experiment performed for our comparative analysis.

3.2 Research Methodology

Our research methodology comprises of following steps

- Research articles related to authentication and encryption schemes were collected. The research articles collected for our research was from 2000 to 2019.These papers were presented/published in conferences and journals during this periods. The total 94 papers were collected, 64 papers were journal papers while 30 were conference papers. With majority of IEEE journal papers.
- We classified the collection of research articles into three classes namely authentication, encryption and survey.

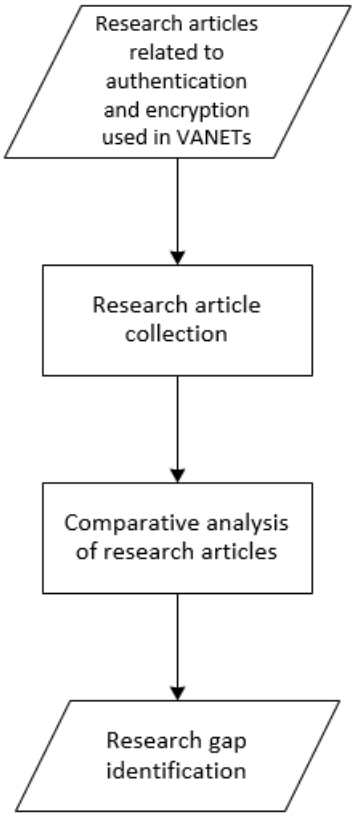

FIGURE 3.1: Research Methodology

- The sources of the research articles were google scholar and citeseerX.
- A comparative analysis of research articles was performed based on performance parameters.
- The data collected in the comparative analysis was used to formulate tables.
- Based on the tables, we then constructed hierarchies of the authentication and encryption schemes.
- Using taxonomies, we identified research gaps in the field of authentication and encryption in VANETs.

3.3 Experiment for Comparative Analysis

For our comparative analysis as stated in the previous section, the research articles related to authentication and encryption schemes were collected and classified into three categories. The research articles were analyzed against performance parameters, strengths, and limitations of the scheme proposed in the research article. The data collected as a result of our analysis, was used to compose the tables. This not only made our research easy but later on proved to be very useful while we constructed hierarchies. **Figure 3.2** and **Figure 3.3** represent the hierarchies of authentication and encryption schemes respectively.
The tabular data helped in identifying the class of authentication or encryption technique to which proposed scheme belonged. The hierarchies were proved to be useful in research gap identification because they highlighted the research deprived areas of respective techniques as well as represented the schemes side by side which was not possible with tables.
Manvi et.al [81] constructed a hierarchy of authentication schemes that are being used in VANETs but Our hierarchy of authentication schemes is different from their work on the following points.

- We identified and mentioned hybrid schemes, whereas their hierarchy doesnt include hybrid schemes.
- We classified encryption-based authentication into two classes whereas they classified encryption-based encryption in three classes.
- We classified asymmetric encryption-based authentication in four classes, whereas they classified asymmetric encryption techniques into two classes.
- We mentioned the surveyed techniques in the hierarchy, but their hierarchy doesnt include and technique.

In the following section we will explain our hierarchies of authentication and encryption schemes.

In hierarchy of the authentication schemes, the authentication schemes are divided into three classes which are named signature based, verification based, and encryption based. In verification based authentication, the vehicle first sends its credentials to RSU which are verified using CA. after verification from CA, RSU verifies the vehicle itself whenever the vehicle communicates with or within the coverage area of the same RSU.

In the digital signature, the message is encrypted using its private key. On the receiver side, this message is decrypted using the senders public key. This process ensures that the message came from the original sender and the message remained unaltered.

While in a digital certificate, the sender sends its certificate to the receiver. On receiving the certificate, the receiver forwards the certificate to certification authority which uses the public key to verify the signature and hence the sender is verified.

Both digital signatures and digital certificates rely on the public key, so technically they are computationally the same. An overlapping relation exists between the digital certificate and digital signatures.

In the hierarchy of encryption schemes, the encryption schemes are classified into two classes namely reversible encryption and irreversible encryption. The term reversible encryption refers to the retrieval of the original text from the encrypted text (ciphertext) when it is decrypted. Whereas the term irreversible encryption refers to the inability to retrieve the original text from the encrypted text (ciphertext). Hash algorithms, generate hash code when they are fed with the message. From this code, the original message cannot be retrieved. Whereas, in other encryption types like asymmetric or symmetric the original message can be retrieved from the encrypted text (ciphertext).

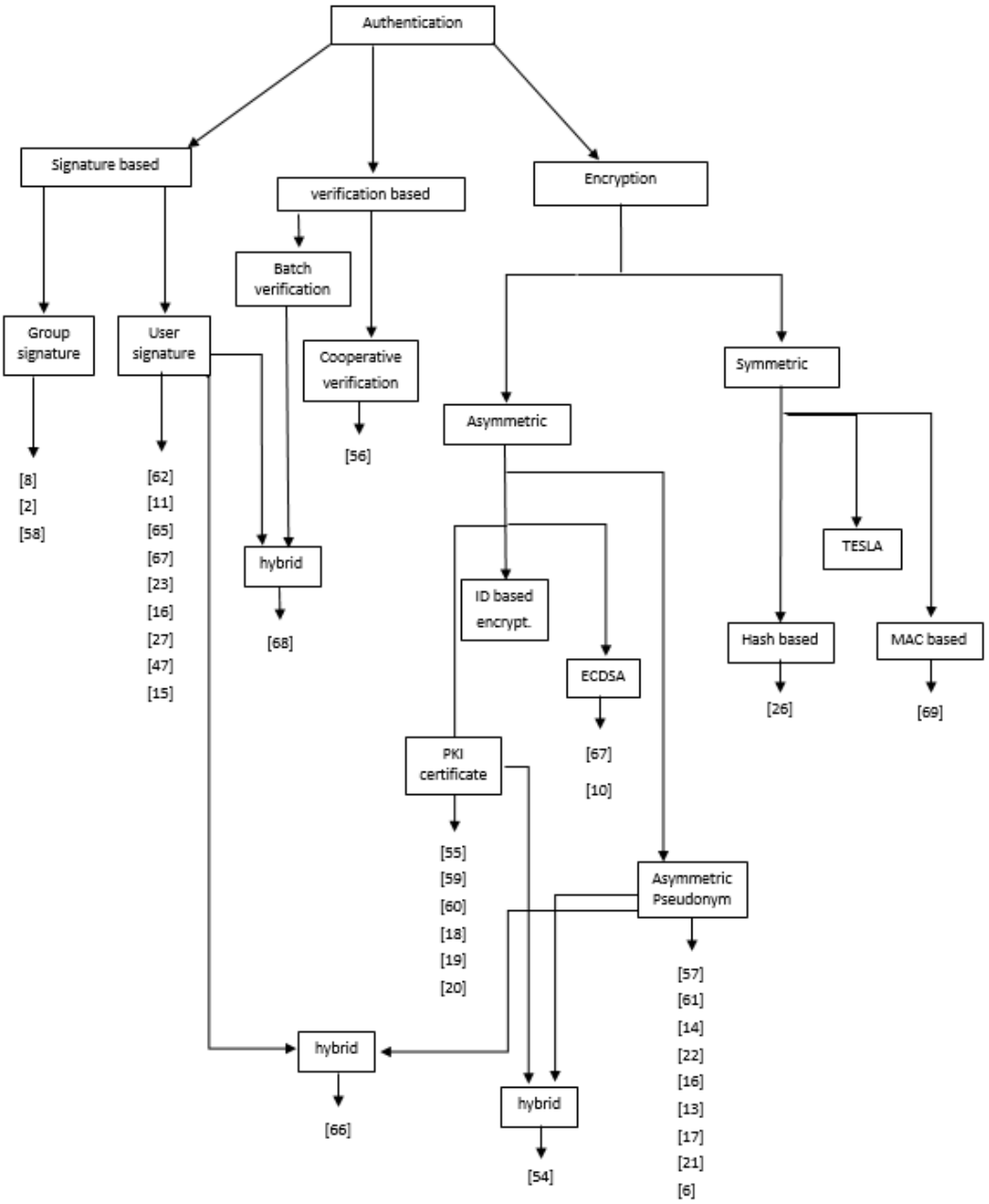

FIGURE 3.2: Taxonomy of Authentication Schemes

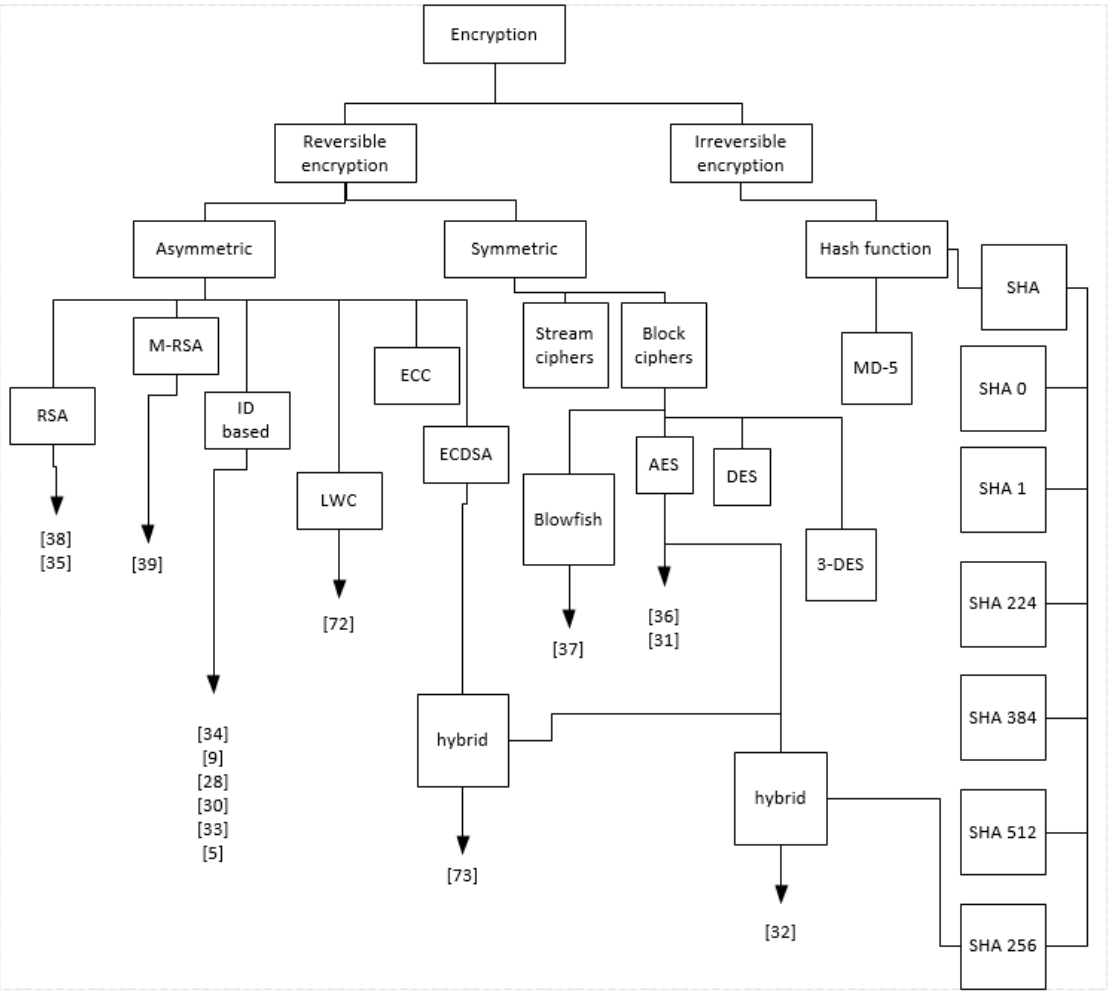

FIGURE 3.3: Taxonomy of Encryption Schemes

Chapter 4

Findings and Results

4.1 Introduction

In this chapter we will present the information about the findings and quantitative results from our experiment explained in previous chapter. the results will be in the form of graphs, which will represent the research gaps in the domain of authentication and encryption schemes in VANETs. The existing surveys lacked the tabular layout of the schemes. Using the tabular layout, we constructed taxonomies of the authentication and encryption schemes (in chapter 3). These taxonomies are the basis of our findings and results.

4.2 Tabular Structure of Comparative Analysis

In this section we will represent comparative analysis in structured form by using tabular layout which are in the form of tables. **Table 1** represents table of authentication schemes while **Table 2** and **Table 3** represents table of encryption schemes and survey of schemes respectively.
Comparative analysis of authentication schemes was conducted on the basis of following parameters

1. Authentication function
2. Authentication type
3. Message size
4. Confidentiality
5. Characteristic of the scheme
6. Authentication direction

A brief description of these parameters is as follows

1. Authentication Function: This parameter indicates which authentication function is used to authenticate the message sender.

2. Authentication Type: This parameter represents which authentication type is being used by the authentication scheme.

3. Message Size: This parameter indicates the size of message a scheme can authenticate.

4. Confidentiality: This parameter represents what information is used in the communication process instead of real identity of the used. The surveyed techniques either have used signatures or pseudonyms instead of real identity of a user.

5. Characteristic of the Scheme: This parameter represents the property of the scheme which makes it different from other schemes.

6. Authentication Direction: This parameter represents the flow of authentication process. If only one of the two entities verifies other entity, then this will be called as one-way authentication. Whereas if both entities authenticate each other, then this authentication flow will be known as two-way authentication.

Comparative analysis of encryption schemes was conducted on the basis of following parameters

1. Cryptographic algorithm
2. Parameters used for cipher text
3. Privacy

4. Characteristics

A brief description of these parameters is as follows

1. Cryptographic Algorithm: This parameter represents that the surveyed technique is using which encryption algorithm.

2. Parameters used for Cipher text: This parameter represents which attributes are used by the encryption algorithm to produce cipher text.

3. Privacy: This parameter represents the information used for communication instead of real identity.

4. Characteristic of the Scheme: This parameter represents the property of the scheme which makes it different from other schemes.

Comparative analysis of survey was conducted on the basis of following parameters.

1. Parameters
2. Objectives
3. Findings

A brief description of these parameters is as follows

1. Parameters: This parameter represents on which attributes survey was conducted.

2. Objectives: This parameter represents what was the objective of the survey.

3. Findings: This parameter represents what was the findings of the authors as a result of their survey.

The following table represents the structured analysis of authentication schemes of VANETs in the tabular format.

TABLE 4.1: Authentication Schemes

Tech.	**Confident.**	**Authen.**	**Auth. scheme**	**Msg. size**	**Charac.**	**Auth. direction**
[59]	Digital signature	Pseudonym and signature based	Hash function	244 bytes	Time stamping of message	Two way
[60]	Elliptic Curve based on Chameleon Hashing	Certificate based	Hash function	NA	1.No info. about previous session is exposed 2. 12.86ms delay for message authentication per 100 vehicle	Two way
[61]	NA	Signature based	NA	NA	300ms verification time per 25 messages	One way
[62]	Crypto. hash function	Pseudonym based	Crypto. Hash function	Any size message	.0004ms time required for authentication	One way
[63]	NA	Group pair key (private and public)	HMAC	NA	Messages are time stamped	One way

[64]	Chaotic cryptography and DBMS based	Certificate and time based	Hash function	NA	1.Ambulances are of highest priority 2. DBMS is used for authentication	One way
65	RSA and DBMS based	Certificate and Nonce based	Hash function	NA	1.Vehicles are categorized 2.Revocation lists are not stored on RSUs but in AAA server	One way
[66]	Pseudonym based (Conditional privacy)	Pseudonym based	Hash function	NA	Important keys like TA key is stored in RSU	Two way
[67]	Group Certificate and Pseudonym based (Conditional privacy)	Signature based	Hash function	935 bytes	Messages are time stamp Synchronization in RSU range is required	One way

[68]	Nonce and key based	Password and Identity based	Hash function	584 bytes	Messages are time stamped 2. 0.2616ms time for message	Two way
[11]	Pseudonym based (Conditional privacy)	Signature based	Crypto. Hash function	NA	verification takes 58.86ms	One way
[69]	Signcrypt	Group signature	Crypto. Hash function	474 bytes	1.RSU maintained groups 2.Batch certificate verification	One way
[19]	Periodical Pseudonym change	Pseudonym based	Encryption based	1024 bytes	Pseudonym change every 30sec	One way
[70]	Key pair based	Signature based	Encryption based	NA	Emergency keys for emergency cases	Two way
[71]	Pseudonym based	Pseudonym and signature	Crypto. Hash function	146 bytes	1.Msgs are timestamped 2.Pseudonm expiration time 30 days	Two way

[72]	Signature based	ECDSA with ID based signature	MAC	128 bytes	No third party certificate required	One way
[23]	Pseudonym based	Certificate based	Hash function	NA	Keys are generated by nodes	Two way
[8]	Pseudonym based	Group signature based	NA	393 bytes for V2V, 281 bytes for V2I	1.Messages are timestamped 2.Mechanism to avoid Sybil attack 3.msg. verification takes 0.8ms	One way
[28]	RSA signature	Signature based	Hash function	746 bytes	1.Three levels of privacy 2.authentication time of .26ms	Two way
[73]	Pseudonym based	Batch Signature based	Hash function	43 bytes	1. messages are time stamped 2. 7.26 ms for message authentication	One way

[24]	DB of vehicle maintained by Law Enforcing Agency	Certificate based	Hash function	NA	Keys are generated by the vehicle itself	One way
20	Group Signature and Id-Based Signature	Signature based	Hash function	NA	1.RSUs act as CA 2. messages are time stamped	Two way
[12]	Pseudonym based	Pseudo-identity	Hash function‘	43 bytes	1.TPD is divided into 4 modules 2. key management center is single point of failure	Two way
74	NA	lightweight hashing process and a fast MAC	MAC and hash function	47 bytes	1.Decentr. model for VANET is suggested 2. biological passwords are used	Two way

[26]	NA	Identity/ pseudonym based	Hash function	NA	No Hash or cryptosys- tem used to reduce com- putational cost	Two way
[27]	Base pseudonym and short time pseudonm.	Pseudonm. based	NA	Less than 500 bytes	1.Pseudo. have life time 2.Two types of pseudonym used	Two way
[29]	Identity of a vehicle is known to Member Manager only	Ring sig- nature based	Hash function	NA	1.Msgs are time stamped 2.Vehicle groups are made by vehicles	One way
[30]	NA	EC-based chameleon hash sig- nature	Hash function	NA	Signature generation is independent of receiver	One way
[15]	Pseudonm based	ECDSA signature based	Hash function	NA	Before send- ing a message distance of destination is determined	One way

[31]	NA	Keyed Hash Message Authentication Code	201 bytes	NA	1.CRL is replaced 2. time stamping is performed	Two way
[32]	Pseudonym based	Signature based	NA	NA	Certificate revocation list CRL is replaced	One way
[63]	Group Identity	Group signature	Keyed hash function	NA	messages are time stamp scheme is resilient towards man in the middle attack	One way
[75]	Pseudonym based	Certificate based	NA	NA	Every entity maintains a server like body called PA of its own	One way
[76]	Private and traceable key	Signature based	Hash function	NA	No pseudonym /certificates are required	One way

[21]	Pseudo-identity based	Pseudonym based	Hash function	NA	Msgs. are time stamped and Group key change offers backward and forward security	Two way
[18]	Pseudonym based	Pseudonym based	Hash function	NA	Changing pseudonyms cannot be linked to previous pseudonym. Neighbor set is formed	One way
[22]	ID based and symmetric encryption	Pseudonym based	Hash function	NA	Broadcasted message will be decrypted within the coverage area of same RSU	Two way

The above table represents the analysis of authentication schemes. We concluded that, most of the techniques provide two way authentication. Most of the techniques time stamp the message before transmission to prevent replay attack. In most of the techniques authentication of message source was performed using Pseudonyms which ensures that true identity of the user remains protected. Use of pseudonym provides conditional privacy which means that true identity of the

user can be retrieved from pseudonym in case of a dispute or suspicious actions.

The following table represents the structured analysis of encryption schemes of VANETs in the tabular format.

TABLE 4.2: Encryption Schemes

Paper	**Encryption algorithm**	**Parameters used for cipher text**	**Privacy**	**Characteristics of the scheme**
[11]	ID based encryption	Pseudonym + message + Hash algorithm	Pseudonym based	Latency is better than ECC based scheme called efficient conditional privacy preservation protocol (ECPP)
[14]	ID based encryption	Publicly available info (Email, etc) and Private key from PKG	PKI	No need for centralized repository or certification authority
[14]	Asymmetric encryption	Public-Private keys and Certificate	PKI based	HASH is used instead of digital signature
[33]	ID based encryption	License + registration number	conditional	No certificates Blow fish encryption scheme is used in IDBC

[77]	Light weight encryption device (LED)	NA	Nil	64 bits block size. For 64 bit and 128 bits version 32 and 48 rounds Less computation required than ECC
[34]	AES+SHA256	Message encrypted using public key then its hash is calculated	Encryption based on AES	Block size of 128 bits with 128/192/256 bits key size No certificates are requires
[78]	ECDSA+ Symmetric Encryption	Message + Hash algorithm + ECC engine for signature + Symmetric Encryption	NA	Light weight and faster than other algorithms but no simulation data was provided
[36]	Symmetric Encryption	Geographical location based key + GPS coordinates	Location based	Vehicle should be physically present to decrypt message in that location whom geo location key is used to encrypt the message
[37]	Symmetric/Asym. depending on the case either V2V or V2I	Public encryption key + signature + private signature key	Pseudonym based	Messages are timestamped before sending

[38]	ID based encryption	Identity of the vehicle Authority + private key from Trusted	Pseudonym based	Messages are time stamped
[79]	Ciphertext-Policy Attribute Based Encryption (CP-ABE)	Public key + An Access Structure	NA	Private key is divided into 2 parts 1 is called Attribute key and other is called secret key
[78]	ID based encryption	Identity+ two certificates of source+ seq. no.+ time to live	Pseudonym based	Most of the comms. between RSU and OBU is based on request and response. (path info)
[41]	Symmetric encryption	Symmetric key + message	Pseudonym based	Messages are time stamped Communication and key exchange are separated from each other
[40]	Asymmetric encryption	Public key + message	Vehicle number + road pass number	Data related to vehicles and road segments is collected
[42]	Blowfish based encryption	Message	NA	64 bits block for encryption XOR operation is the main operation performed in every phase of the algorithm

[43]	Asymmetric encryption	Message+ public key of receiver + time stamp	Signature based	Message are time stamped Safety messages are not encrypted Challenge and response model with RTT based connection
[39]	ID based encryption	Msg+receivers public key+ RSUs public key	Signature based	This scheme defines four phases of communication in VANETs. Smaller computational time then other id-based cryptographic schemes.
[44]	Modified RSA	Message+ public key	NA	MRSA out performs RSA in decryption and encryption time with same size of key and data. MRSA provides enhanced security.

The above table represents the analysis of encryption schemes. We concluded that, most of the techniques used Identity based encryption. The advantage of identity based encryption is that it uses publicly known parameters for encryption and decryption. The public key of message source is retrieved from Public Key Generator(PKG). This not only provides security but provides authentication of message source as well. The majority of techniques provided pseudonym based privacy. Using pseudonyms provides security and privacy but also provides

a mechanism for resolution of disputes and accountability for malicious activities. Few techniques time stamped the message before transmission.

The following table represents the structured analysis of existing survey of VANETs in the tabular format.

TABLE 4.3: Existing Surveys

Paper	**Survey**	**Parameters**	**Objectives**	**Findings**
[45]	Survey on Security and privacy based on Cryptography	Privacy and anonymity approaches	Compare existing privacy techniques and highlight their pros and cons	Tradeoff between security and privacy. For security, there is a compromise on privacy
[46]	Survey on authentication	Authentication methods	Issues regarding authentication and digital signature.	Field of authentication requires research for an efficient and low computation cost algorithm.
[47]	Survey on Security	Security services and threats	Provide overview of treats and security services	Many important aspect of VANETsecurity is not discussed by research community
[48]	Survey on User Authentication	Authentication protocols	Position of the user to be used in authentication process.	Security primitives for VANETs were not considered. Threats to be considered that are associated with wireless communication.

[49]	Survey on Security	Security threats, requirements and solutions	Security related issues	Security threats, attack and attackers identified
[10]	Survey on Security	Attacks, security challenges and requirements	Review existing security solutions and categorize them	There exist not a single security mechanism which resolves all possible security issue know to literature
[7]	Survey on VANET security and comms. architecture on basis of Cryptography	Attacks, cryptographic techniques	Comparison of cryptographic schemes in VANETs	Security problems were analyzed cryptographic point of view and Cryptographic solution to these problem suggested
[50]	Survey on Cryptographic solution	Cryptographic schemes, security challenges	Overview of proposed cryptographic solutions	New cryptographic techniques like ID-based, homomorphic encryption techniques are not used
[52]	Survey on Security	Attacks, security solutions	Overview of attacks and security solutions	VANET security is a major concern

[51]	Survey on Security	Security techniques and attacks	Discuss the available techniques ability to provide security	Cell phone stations to be used as RSUs to facilitate cost effective communication
[53]	Survey on Security and Privacy	Security issues, solutions to issues, privacy solutions	Discuss the security, privacy issues and tradeoff between the two	Trade of between security and privacy. All attention of research community is towards Authentication protocols.
[54]	Survey of authentication schemes	Authentication schemes	Overview of authentication schemes and their comparison	Authentication still requires a lot of research
[55]	Survey on security and privacy approaches	Cryptographic techniques	Security and privacy issues in VANETs and their solutions	Cryptographic techniques provide security and privacy
[56]	Survey on security	Cryptographic algorithm RSA and ECC	Compare RSA and ECC algo and identify their limitations and advantages	For short messages RSA out performs ECC but for longer messages ECC is better

[80]	Survey of cryptographic techniques in VANETs	Cryptographic techniques	Identify a scheme that provides security and privacy desired	ECC is faster in encryption and RSA is faster in decryption.
[57]	Survey of authentication and privacy schemes	Authentication and privacy schemes	Identify limitations and strengths of these schemes	Open issues like trade-off between safety and privacy identified
[58]	Survey on security services	Attacks, their counter measures and authentication schemes	Identify security challenges and indicate possible solutions	Privacy is the major concern of rivers and passengers. An algorithm is required for privacy protection

The above table represents the analysis of existing surveys. Majority of the existing surveys analyzed the security threats and attacks on VANETs. The objectives of these studies were to provide overview of the security services and classification of attacks. Few studies compared cryptographic schemes used in VANETs with comparison of these schemes as an objective.

4.3 Findings

In this section, we will present our findings followed by detail explanation of our findings. Based on our comparative analysis, the following are our findings

- In authentication schemes, encryption-based authentication is widely used. In encryption-based authentication, asymmetric encryption is widely used.
- In asymmetric encryption-based authentication, an asymmetric Pseudonym scheme is widely used.
- Verification based authentication is the least used scheme for authentication.
- In encryption schemes, reversible encryption is widely used. In reversible encryption, Asymmetric encryption is widely used.
- In asymmetric encryption, ID-based encryption is widely used.
- An overlapping relationship exists between the digital certificate and the digital signature schemes.
- Very few hybrid schemes exist for authentication and encryption.
- No encryption scheme uses elliptic curve cryptography.
- No authentication scheme uses ID based encryption for authentication.

In following section, we will explain our findings.
In ID based encryption, verifier use a publically know information for the verification of the message source. This information could be an email Id, phone number or could be combination of anything which can be used to identify a user. This information is use to retrieve public key of the sender which is provided by the PKG (public key generator). PKG will not be accessed until the key is renewed or new entities enter into the network. This feature removes the need of a central authority used to authenticate message source like incase of digital signature or digital certificate. Thus saving bandwidth and time which makes it ideal for use in VANETs for authentication. [72][14].
In Digital signature, the public key of every entity is known throughout the network. Whenever message is sent, source encrypts the message using its private key. The receiver uses the public key of sender to decrypt the message.
In case of digital certificate, every network entity registers its public key to CA

(Central Authority). CA generates the certificate for each public key and provides it to the key owner. Whenever a message is sent, sender attaches its certificate with the message. The receiver sends the received certificate to CA which authenticates the message source.

So in both Digital signature and Digital certificate, the public key is used to authenticate the message source which indicates that computationally an overlapping relationship between digital certificate and digital signature.

Lightweight encryption schemes could be used for encryption in VANETs. Because Lightweight encryption schemes are used in environment that suffer from limited sources like throughput or speed, memory or computing resources. VANETs being resource limited network suffering from limited storage, low processing makes it an ideal contender for lightweight encryption schemes[81][82] [2][7]. Lightweight encryption schemes like PRESENT which is proposed as a replacement of AES. PHOTON is lightweight encryption algorithm based on AES[17]. So lightweight encryption algorithm offer similar or identical performance as of conventional cryptographic methods.

We reviewed 34 authentication schemes and 15 encryption schemes for our research. We identified only 5 hybrid schemes i.e. 3 hybrid schemes were identified in authentication schemes and 2 hybrid schemes were identified in encryption schemes.

In our survey of authentication and encryption schemes, we identified that either in case of authentication or in case of encryption, no scheme used ECC (elliptic curve cryptography). Only one scheme used ECDSA (Elliptic Curve Digital Signature Algorithm). ECC provides strong security with fast encryption and decryption times[80]. ECC requiring less computation power, storage, bandwidth and power consumption. ECC being resource efficient, we suggest ECC could be used in its true essence for VANET security[83].

We classified the encryption schemes into two classes namely, reversible and irreversible encryption schemes. For our survey of encryption schemes, we reviewed 15 encryption schemes. Out of 15, 13 were reversible encryption schemes. 2 schemes

were hybrid schemes while no scheme used irreversible encryption. In reversible encryption, 10 schemes were asymmetric encryption schemes while 3 schemes were symmetric encryption techniques. So, we concluded that reversible encryption class with asymmetric encryptions are widely used for encryption in VANETs.

4.4 Results

In this section, we will discuss the results from our comparative analysis of authentication, encryption schemes in the form of graphs.
For the analysis of authentication schemes, 34 techniques were reviewed. Out of 34 techniques, 18 techniques used encryption based authentication. 12 techniques used signature based authentication while 3 techniques were hybrid technique and 1 technique used verification based authentication. **Figure 4.1** represents the survey of authentication schemes used in VANETs. The Hybrid techniques were combination of the following techniques

- Signature based and Batch verification based.
- Signature based and Pseudonym based.
- Certificate based and Pseudonym based.

Out of 18 techniques that were using encryption based authentication, 16 techniques used asymmetric encryption while 2 techniques used symmetric encryption authentication. **Figure 4.2** represents the encryption based authentication schemes.

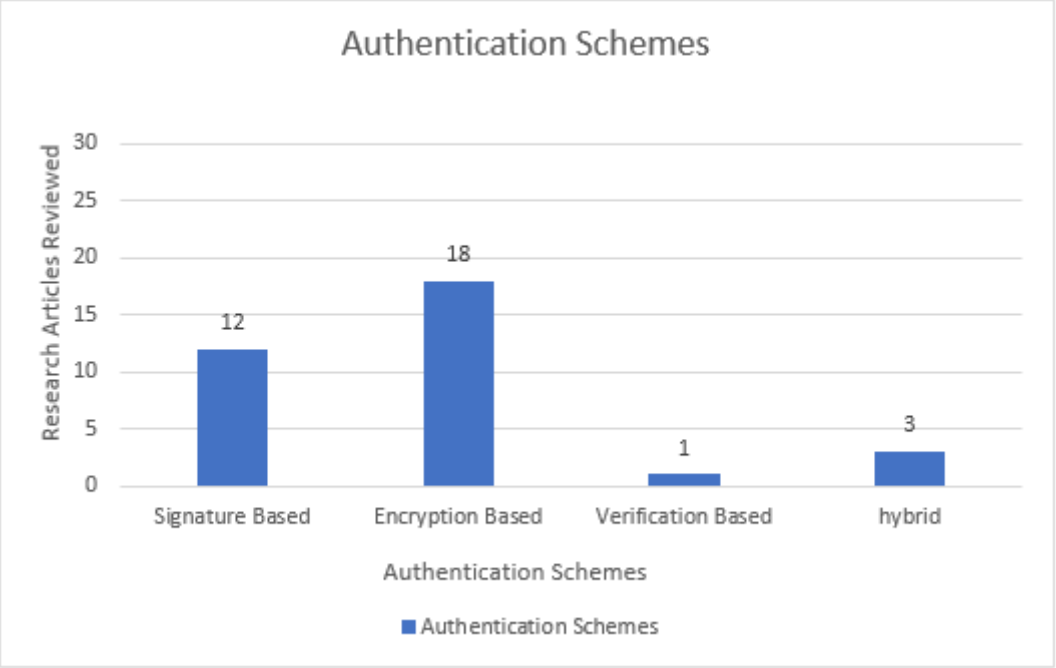

FIGURE 4.1: Authentication Schemes

Out of 16 techniques using asymmetric encryption based authentication, 9 techniques used Pseudonym based encryption, 5 techniques used PKI Certificate based encryption while 2 techniques used ECDSA based encryption. **Figure 4.3** represents the asymmetric encryption based authentication.

12 techniques used signature based authentication. Out of 12, 9 techniques used user signature based authentication while 3 techniques used group signature based authentication. **Figure 4.4** represents the signature based authentication.

From above discussion we concluded that encryption is commonly used for authentication. In encryption based authentication, asymmetric encryption was commonly used. While in asymmetric encryption, Pseudonym based encryption was commonly used.

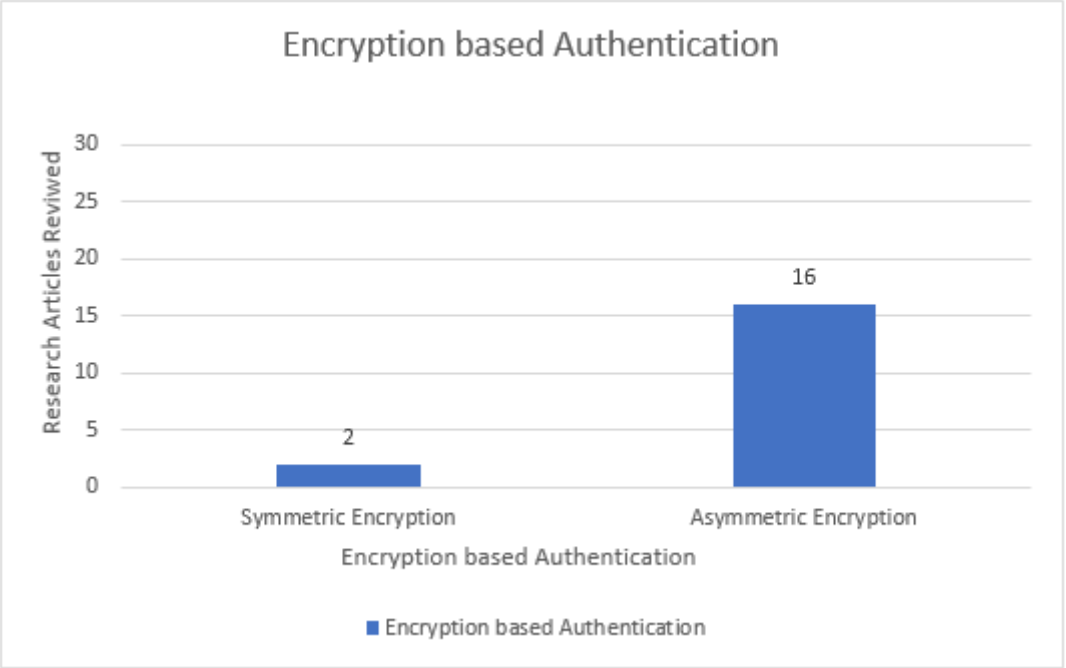

FIGURE 4.2: Encryption based Authentication Schemes

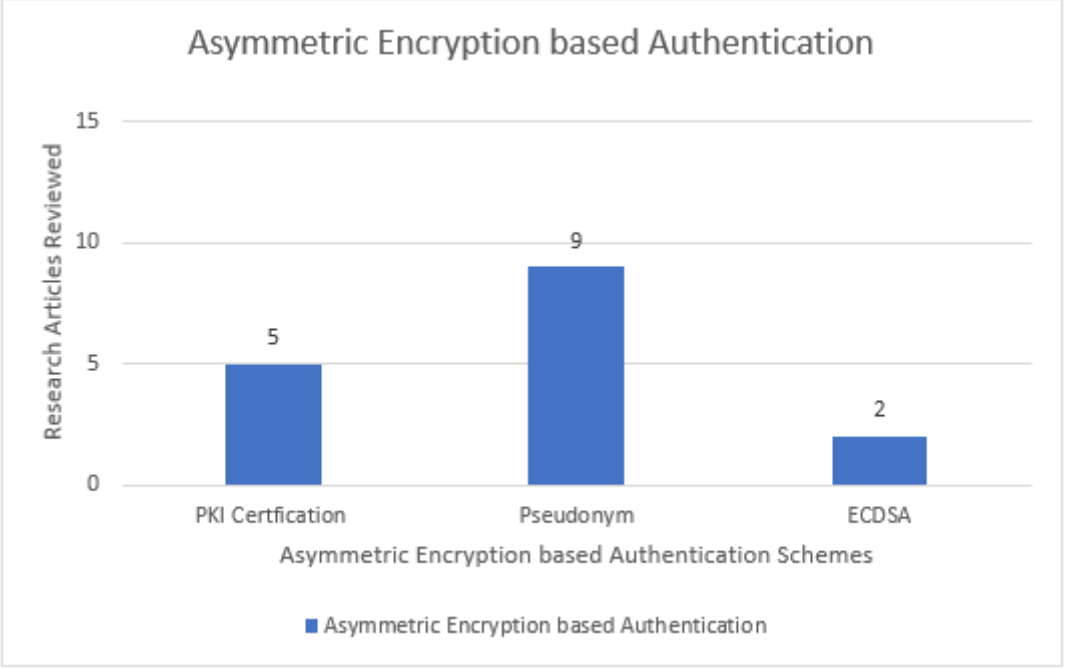

FIGURE 4.3: Asymmetric Encryption based Authentication Schemes

For the analysis of encryption schemes, 15 techniques were reviewed. Encryption schemes were classified into 2 classes. These classes are named as

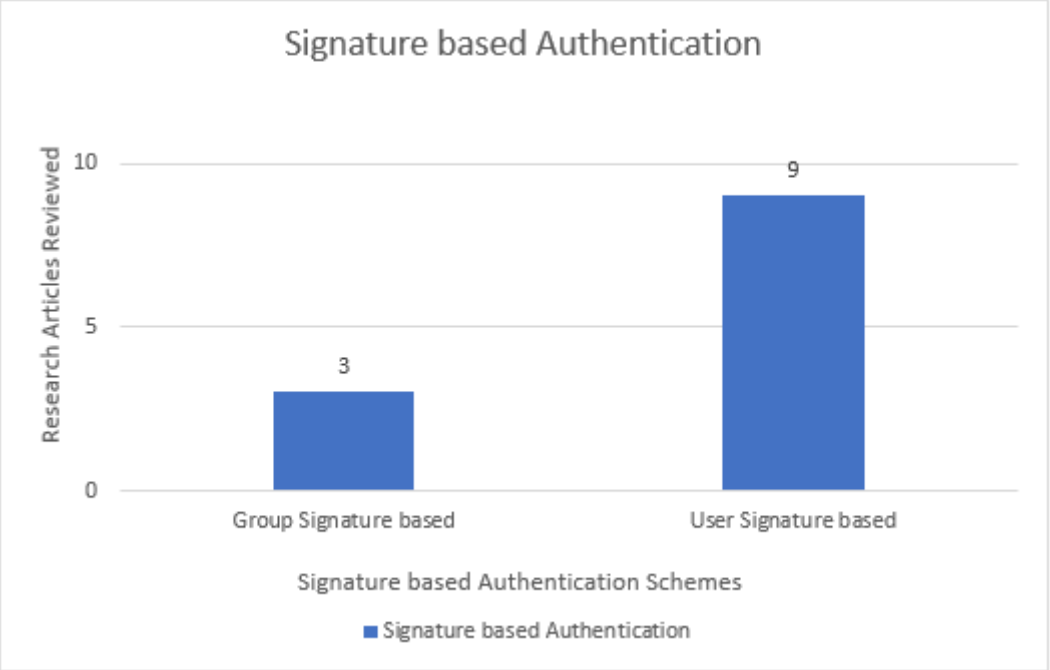

FIGURE 4.4: Signature based Authentication Schemes

- Reversible encryption schemes
- Irreversible encryption schemes

Out of 15 techniques, 13 techniques were reversible encryption schemes while none of the techniques used reversible encryption. **Figure 4.5** represents the analysis of encryption schemes.
2 techniques were hybrid schemes and these schemes were combination of following techniques

- Asymmetric encryption and Symmetric encryption
- Asymmetric encryption and Hash function

Out of 13 techniques that used reversible encryption, 10 techniques used Asymmetric encryption while 3 techniques used Symmetric encryption. Out of 10 Asymmetric encryption techniques, 6 techniques used Identity based encryption, 2 techniques used RSA algorithm while Light weight cryptography and Modified RSA algorithm was used by a single technique each. **Figure 4.6** represents the

Asymmetric encryption schemes. **Figure 4.7** represents the symmetric encryption schemes.

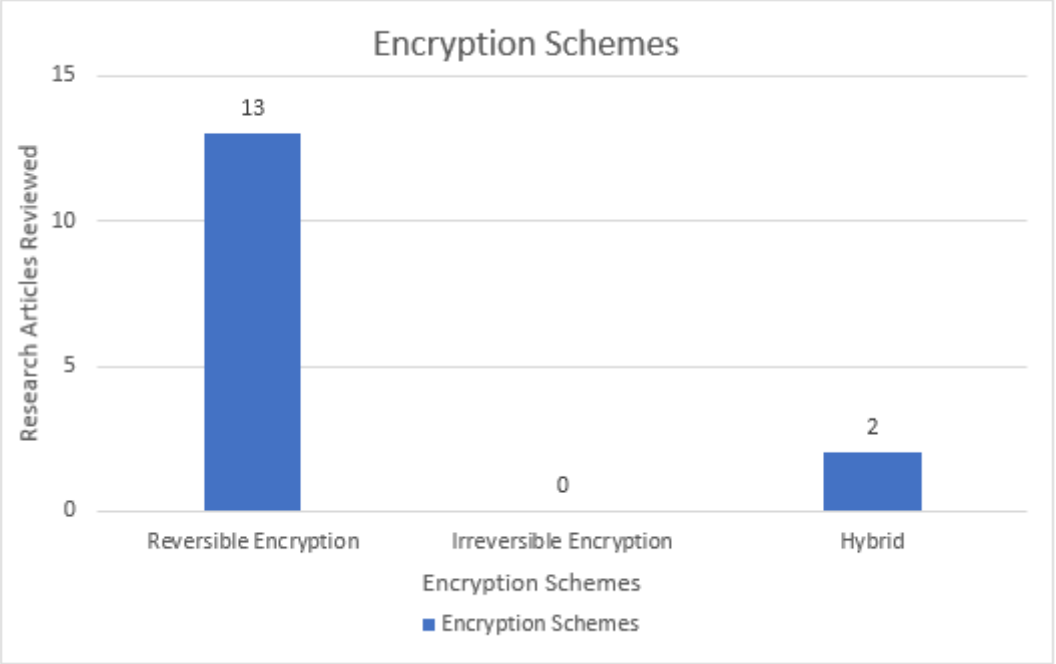

FIGURE 4.5: Encryption Schemes

For the analysis of encryption schemes, we classified the encryption schemes into two classes. That are Reversible and Irreversible encryption schemes. We conclude that most of the analyzed techniques used reversible encryption.

In Reversible encryption, Asymmetric encryption was commonly used. In asymmetric encryption techniques, Identity based encryption was commonly used. Similarly in symmetric encryption techniques, AES algorithm was used.

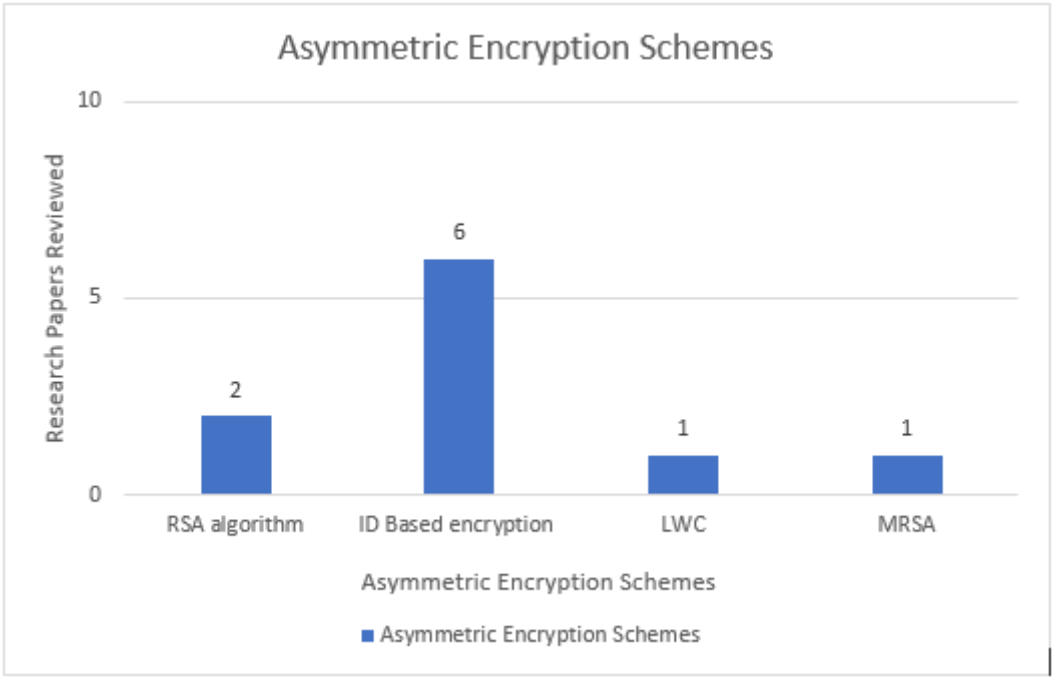

FIGURE 4.6: Asymmetric Encryption Schemes

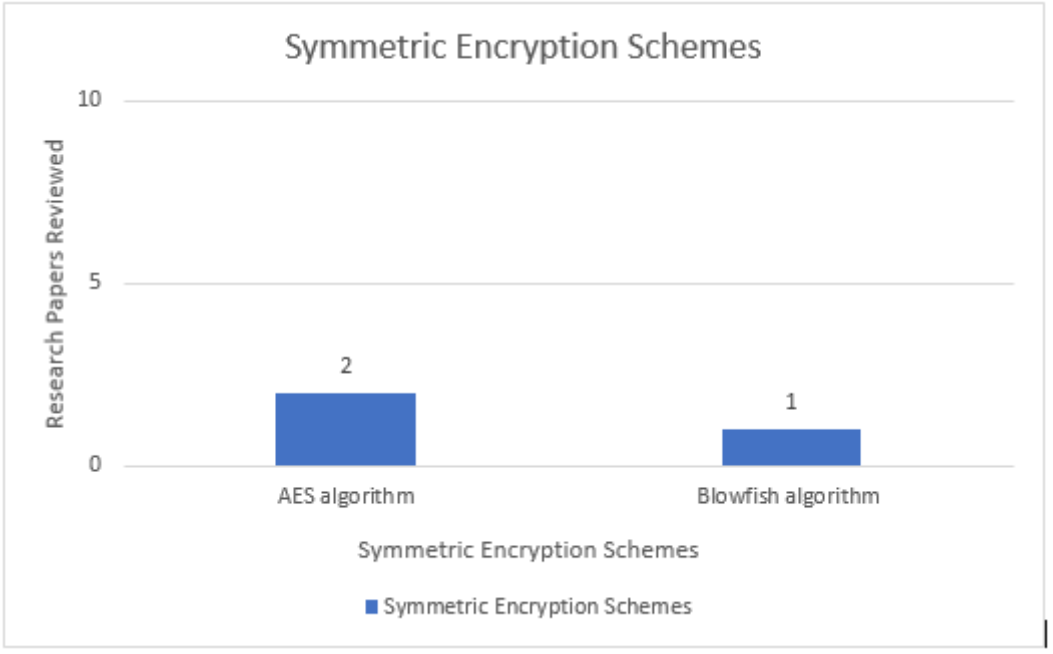

FIGURE 4.7: Symmetric Encryption Schemes

Chapter 5

Conclusion and Future work

5.1 Conclusion

Information security, as well as privacy preservation, is a major requirement in VANETs. For security and privacy, authentication and encryption are used. But with limited resources, VANETs suffer from a tradeoff between security and performance. VANETs being resource-limited, Traditional encryption and authentication schemes cannot be implemented with their true essence because they require large storage and a powerful computing resource. In this paper, we performed a structured analysis of authentication and encryption schemes. Based on our comparative analysis we concluded that

- Lightweight encryption scheme could be used for encryption.
- ID based encryption could be used for authentication purposes.
- There exists a tradeoff between security and performance.
- Elliptic curve cryptography was not used for encryption in any of the surveyed techniques.
- There is a need for hybrid scheme which offers better performance and security that could bridge the gap.

As we have identified that Elliptic curve cryptography to be used for encryption and Identity based cryptography to be used for authentication. These both algorithms offer better performance and security than all other algorithms currently used in VANETs[56][38]. As existing surveys identified a tradeoff between security and performance [57][45][51][54], using these two algorithms can bridge the tradeoff between security and performance.Having said that, there exists a lot of research that needs to be done to enhance the security of VANETs.

5.2 Future Tasks

In the future, we will further enhance our research and will try to propose a scheme that satisfies the security and performance requirements of VANETs. We will refine hierarchies to add new concepts. We will work on schemes related to availability and add to our survey. We will refine and add new parameters to tabular layout based survey for these schemes

Bibliography

[1] A. Rahim, I. Ahmad, Z. S. Khan, M. Sher, M. Shoaib, A. Javed, and R. Mahmood, "A comparative study of mobile and vehicular adoc networks," *International Journal of Recent Trends in Engineering*, vol. 2, no. 4, p. 195, 2009.

[2] M. S. Sheikh and J. Liang, "A comprehensive survey on vanet security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[3] P. Agarwal, "Technical review on different applications, challenges and security in vanet," *J. Multimed. Technol. Recent Adv*, vol. 4, no. 3, pp. 21–30, 2017.

[4] N. Mathew and V. Uma, "Vanet security-analysis and survey," in *2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT)*. IEEE, 2018, pp. 100–106.

[5] F. Aadil, S. Rizwan, and A. Akram, "Vehicular ad hoc networks (vanets), past present and future: A survey," 2011.

[6] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[7] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[8] T. B. M. de Sales, A. Perkusich, L. M. de Sales, H. O. de Almeida, G. Soares, and M. de Sales, "Asap-v: A privacy-preserving authentication and sybil detection protocol for vanets," *Information Sciences*, vol. 372, pp. 208 – 224, 2016.

[9] S. Biswas and J. Mii, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, Jun 2013.

[10] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2013, pp. 59–74.

[11] D. Huang, S. Misra, M. Verma, and G. Xue, "Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[12] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "Lespp: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication," *Computing*, vol. 98, no. 7, pp. 685–708, 2016.

[13] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2009.

[14] G. Baldini, V. Mahieu, I. N. Fovino, A. Trombetta, and M. Taddeo, "Identity-based security systems for vehicular ad-hoc networks," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2013, pp. 672–678.

[15] B. Mishra, S. K. Panigrahy, T. C. Tripathy, D. Jena, and S. K. Jena, "A secure and efficient message authentication protocol for vanets with privacy preservation," in *2011 World Congress on Information and Communication Technologies*. IEEE, 2011, pp. 880–885.

[16] A. O. Bayrak and T. Acarman, "A secure and privacy protecting protocol for vanet," in *2010 IEEE Intelligent Vehicles Symposium*. IEEE, 2010, pp. 579–584.

[17] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 187–201, 2017.

[18] M. Zeng and H. Xu, "Mix-context-based pseudonym changing privacy preserving authentication in vanets," *Mobile Information Systems*, vol. 2019, 2019.

[19] A. Adigun, B. A. Bensaber, and I. Biskri, "Protocol of change pseudonyms for vanets," in *38th Annual IEEE Conference on Local Computer Networks - Workshops*, Oct 2013, pp. 162–167.

[20] M. B. Younes and A. Boukerche, "Scool: A secure traffic congestion control protocol for vanets," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2015, pp. 1960–1965.

[21] L. Liu, Y. Wang, J. Zhang, and Q. Yang, "A secure and efficient group key agreement scheme for vanet," *Sensors*, vol. 19, no. 3, p. 482, 2019.

[22] B. Wang, Y. Wang, and R. Chen, "A practical authentication framework for vanets," *Security and Communication Networks*, vol. 2019, 2019.

[23] C. Caballero-Gil, P. Caballero-Gil, and J. Molina-Gil, "Mutual authentication in self-organized vanets," *Computer Standards & Interfaces*, vol. 36, no. 4, pp. 704 – 710, 2014, security in Information Systems: Advances and new Challenges.

[24] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Bars: A blockchain-based anonymous reputation system for trust management in vanets," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug 2018, pp. 98–103.

[25] V. Casola, J. Luna, A. Mazzeo, M. Medina, M. Rak, and J. Serna, "An interoperability system for authentication and authorisation in vanets," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 3, no. 2, pp. 115–135, 2010.

[26] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for vanet by using digital certification to provide security with low bandwidth," in *2014 International Conference on Communication and Signal Processing*. IEEE, 2014, pp. 768–772.

[27] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for vanet," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2015, pp. 643–650.

[28] C. Fan, W. Sun, S. Huang, W. Juang, and J. Huang, "Strongly privacy-preserving communication protocol for vanets," in *2014 Ninth Asia Joint Conference on Information Security*, Sep. 2014, pp. 119–126.

[29] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for vanet," *Computers & Electrical Engineering*, vol. 38, no. 3, pp. 573–581, 2012.

[30] A.-N. Shen, S. Guo, D. Zeng, and M. Guizani, "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2012, pp. 2543–2548.

[31] A. Wasef and X. Shen, "Emap: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, Jan 2013.

[32] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for vanet," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[33] C. Y. Yeun, M. Al-Qutayri, and F. Al-Hawi, "Efficient security implementation for emerging vanets," *UbiCC J*, vol. 4.

[34] S. S. Karanki and M. S. Khan, "Smmv: Secure multimedia delivery in vehicles using roadside infrastructure," *Vehicular Communications*, vol. 7, pp. 40–50, 2017.

[35] C. Wang, D. Shi, X. Xu, and J. Fang, "An anonymous data access scheme for vanet using pseudonym-based cryptography," *Journal of Ambient Intelligence and Humanized Computing*, vol. 7, no. 1, pp. 63–71, 2016.

[36] G. Yan, S. Olariu, and M. C. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 16, no. 6, pp. 48–55, 2009.

[37] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE, 2008, pp. 508–513.

[38] W. Cho, Y. Park, C. Sur, and K. H. Rhee, "An improved privacy-preserving navigation protocol in {VANET} s." *JoWUA*, vol. 4, no. 4, pp. 80–92, 2013.

[39] F. Zhou, Y. Li, and Y. Ding, "Practical v2i secure communication schemes for heterogeneous vanets," *Applied Sciences*, vol. 9, no. 15, p. 3131, 2019.

[40] A. Malik and B. Pandey, "Asymmetric encryption based secure and efficient data gathering technique in vanet," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*. IEEE, 2017, pp. 369–372.

[41] L. Zhu, C. Chen, X. Wang, and A. O. Lim, "Smss: Symmetric-masquerade security scheme for vanets," in *2011 Tenth International Symposium on Autonomous Decentralized Systems*. IEEE, 2011, pp. 617–622.

[42] G. Anitha and K. GnanaSelvi, "Data security in vanet dissemination using advanced cryptographic techniques," *International Journal of Science, Engineering and Management (IJSEM)*, vol. 2, 2017.

[43] R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, "Improving vehicular authentication in vanet using cryptography," *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 248–255, 2018.

[44] D. Roy and P. Das, "A modified rsa cryptography algorithm for security enhancement in vehicular ad hoc networks," in *Proceedings of the International Conference on Computing and Communication Systems*. Springer, 2018, pp. 641–653.

[45] S. Biswas, M. M. Haque, and J. V. Misic, "Privacy and anonymity in vanets: A contemporary study." *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 2-3, pp. 177–192, 2010.

[46] K. Haseeb, M. Arshad, S. Yasin, and N. Abbas, "A survey of vanets authentication," *Islamia College Peshawar, Pakistan*, 2010.

[47] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in vanet security: a survey," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*. IEEE, 2015, pp. 1–7.

[48] A. Dahiya and V. Sharma, "A survey on securing user authentication in vehicular ad hoc networks," *International Journal of Information Security*, vol. 1, pp. 164–171, 2001.

[49] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[50] M. N. Mejri and M. Hamdi, "Recent advances in cryptographic solutions for vehicular networks," in *2015 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2015, pp. 1–7.

[51] M. A. Moharrum and A. A. Al-Daraiseh, "Toward secure vehicular ad-hoc networks: a survey," *IETE Technical Review*, vol. 29, no. 1, pp. 80–89, 2012.

[52] R. Mishra, A. Singh, and R. Kumar, "Vanet security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016, pp. 1050–1055.

[53] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[54] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, no. 10, pp. 1137–1152, 2011.

[55] V. Sahare, M. Sarode, and N. Sahare, "A survey on security and privacy approaches of intelligent vehicular ad-hoc network (invanet)," 2017.

[56] R. Shaikh and D. Deotale, "A survey on vanet security using ecc, rsa & md5," *International Journal of Advanced Research in Compute and Communication Engineering*, vol. 4, no. 6, pp. 167–172, 2015.

[57] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey," *Vehicular Communications*, 2019.

[58] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[59] N. B. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. Ur Rahman, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31 808–31 819, 2018.

[60] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2794–2803, Nov 2014.

[61] Y. Hao, T. Han, and Y. Cheng, "A cooperative message authentication protocol in vanets," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 5562–5566.

[62] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets," *Future Generation Computer Systems*, vol. 84, pp. 216 – 227, 2018.

[63] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in vanet," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, Oct 2017, pp. 478–483.

[64] N. Meddeb, A. Makhlouf, and M. A. Ben Ayed, "A multilevel authentication protocol (map) for human safety in vanet," 06 2018, pp. 916–921.

[65] A. Meddeb-Makhlouf, N. Meddeb, and M. A. B. Ayed, "An enhanced multilevel authentication protocol for vanets," in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, Oct 2017, pp. 1232–1238.

[66] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet," *Computer Networks*, vol. 134, pp. 78 – 92, 2018.

[67] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, March 2016.

[68] H. Vasudev and D. Das, "A lightweight authentication protocol for v2v communication in vanets," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2018, pp. 1237–1242.

[69] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[70] A. O. Bayrak and T. Acarman, "A secure and privacy protecting protocol for vanet," in *2010 IEEE Intelligent Vehicles Symposium*, June 2010, pp. 579–584.

[71] N. B. Bhavesh, S. Maity, and R. C. Hansdah, "A protocol for authentication with multiple levels of anonymity (amla) in vanets," in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, March 2013, pp. 462–469.

[72] S. Biswas and J. Mišić, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[73] S. Horng, S. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, Nov 2013.

[74] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, Feb 2016.

[75] V. Casola, J. Luna, A. Mazzeo, M. Medina, M. Rak, and J. Serna, "An interoperability system for authentication and authorisation in vanets," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 3, pp. 115 – 135, 01 2010.

[76] H. Liu, Y. Sun, Y. Xu, R. Xu, and Z. Wei, "A secure lattice-based anonymous authentication scheme for vanets," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 66–73, 2019.

[77] W. Li, V. Rijmen, Z. Tao, Q. Wang, H. Chen, Y. Liu, C. Li, and Y. Liu, "Impossible meet-in-the-middle fault analysis on the led lightweight cipher in vanets," *Science China Information Sciences*, vol. 61, no. 3, p. 032110, 2018.

[78] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "Vanet security framework for trusted grouping using tpm hardware," in *2010 Second International Conference on Communication Software and Networks*. IEEE, 2010, pp. 309–312.

[79] X. Liu, Y. Xia, W. Chen, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "Semd: Secure and efficient message dissemination with policy enforcement in vanet," *Journal of Computer and System Sciences*, vol. 82, no. 8, pp. 1316–1328, 2016.

[80] K. Jashnani and P. P. Sharma, "Comparison of different cryptography approach for secure communication in vehicular ad-hoc network," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, 2016.

[81] H. Zhao, Y. Zhang, H. Zhu, and D. Li, "Resource management in vehicular ad hoc networks: Multi-parameter fuzzy optimization scheme," *Procedia Computer Science*, vol. 129, 2018.

[82] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[83] G. M. De Dormale and J.-J. Quisquater, "High-speed hardware implementations of elliptic curve cryptography: A survey," *Journal of systems architecture*, vol. 53, no. 2-3, pp. 72–84, 2007.