An Efficient Privacy Preserving Protocol for VANET Using Hybrid Approach

Safia Mushtaq, Noor ul Amin, Jawaid Iqbal, Chand Bibi, Yousra Saeed and Irshad Ullah

Department of Information Technology
Hazara University Mansehra
K-P, Pakistan

Abstract

VANET is a subcategory of MANET with unique features of Vehicle-to-Vehicle communication, Vehicle-to-RSU communication and Vehicle-to-Trusted Authority communication. VANET has a dynamic topology. Now-a-days VANET has been ultimately a hot research topic for the researchers and work is in progress for the improvement in this area. However, there is gap found needs to be filled, as in the existing scheme, authors used HECC for both encryption/decryption of data and also for secure key exchange. The existing scheme is more complex due to which, timely data availability is a problem and face problems of node authenticity, non-repudiation and similarly the problem of cost i.e. storage cost, communication cost and also computational cost. In our propose scheme we use a hybrid approach, which contain blowfish algorithm (called symmetric algorithm) and HECC (called asymmetric algorithm). Blowfish algorithm is used for confidentiality i.e. encryption/decryption of data and HECC is used for secure key exchange. The objective of our propose scheme is to securely transmit data among vehicles, RSU and server, and protect various security attacks on VANETs, while keeping in view the efficiency in terms of cost as well as the privacy of messages transmission.

Keywords

Vehicular-Ad-hoc Network (VANET), Hyper Elliptic Curve Cryptography (HECC), Mobile-Ad-hoc Network (MANET), Blowfish, Road Side Unit (RSU), Vehicle-to-Vehicle (V2V), Vehicle-to-RSU (V2R), Vehicle-to-Trusted Authority (V2T).

1. Introduction

Many accidental events occur due to less attention of drivers. Most of the people injure or die in a road accident. About half of the world affect due to the road accident. Accidents can be avoided if the driver gets the notice even before one or half a second of an accident. Traffic jam is another problem for drivers on road. All these challenges are due to less security in VANETs system. There are many attacks that are possible in VANETs system.

VANET is an enhance form of MANET.There are few characteristics of VANET that makes it different from MANET, i.e. High flexibility of nodes, fast changing network topology, infinite network size, possible support from an organization, instantaneous, time-sensitive data exchange and essential result of security and privacy.

VANETs Communication are of three types i.e. Vehicle-to-Vehicle Communication, Vehicle-to-RSU Communication and Vehicle-to-Trusted authority/server Communication. V2V Communication is a wireless communication between vehicles. This communication design is suitable where messages are being sent to a group of vehicles or a particular vehicle. In V2R Communication once a possible attacks are detected, transfer messages are done both through infrastructure for example through RSUs or a vehicle. For the communication between vehicles and RSUs, high bandwidth association is used. V2T communication is that in which vehicles can communicate through wireless broadband devices such as Wi-Fi 3G/4G.

Now-a-days most of the researchers work on the VANET security. Different schemes have been used for VANET security. In traditional identity-based signature structure [1] was to be provided privacy and authentication of V2V communication and V2R of the VANET. Authentication providing cooperative communications, that is from vehicle to RSU and RSU to vehicle. ID-based signature system worked on Elliptic Curve Cryptosystem (ECC) authentication procedure and moreover provided batch message verification mechanism. They discussed the ECC-based structure that requires 160-bits key size to encrypt the message transmitted among vehicle and RSU. ECC-based structure requires large memory space and also consumes more energy and leads to high computational and communication overhead. But they proposed new authentication structure that works on the advantage of HECC to sign the message transmitted among vehicle and RSU, where HECC needs smaller 80-bits key size than the traditional signature system, it deals greater level of security with less computational and communication overhead.

Blowfish was introduced [2] by Bruce Schneider in 1993 as a rapid, free alternative to existing encryption algorithms. Blowfish is a symmetric block cipher, which is worked on encryption/encoding and decryption/decoding. It has key length from 32 bits to 448 bits for obtaining a secure data. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Each line has 32 bits. Algorithm preserves two sub-key arrays i.e. the 18-Entry P-Array four 256-Entry S-Boxes. S-Boxes take 8-bits

Manuscript received February 5, 2019
Manuscript revised February 20, 2019

input and produce 32-bits output. One entry of P-Array is used for each round. After last round, every half of data block is XOR with one of the two remaining idle P-Entries. The blowfish algorithm works on data in large blocks has a 64-bit block size. It has an accessible key, from 32 bits to the minimum 256 bits. It works on simple operations, which are efficient on microprocessors i.e. XOR, addition, table lookup and modular multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps. Works precomputable sub keys. Blowfish encryption algorithm wants 32 bits microprocessor at a rate of 1 byte for each 26 clock cycles. Blowfish consists of 16 rounds. Every round contains of XOR operation and a function. Every round contains of key expansion and data encryption. Key expansion usually worked for creating initial substances of one array and data encryption uses a 16 round Feistel network procedures. Fig.1 displays that how blowfish algorithm is working. Key and plain text are the inputs of this algorithm, 64 bits plain text occupied is divided into two 32 bits data and at every round the given key is extended and deposited in 18 P-Array and provides 32 bits key as input and XOR with previous round data.

Then, for i = 1 to 16:

$X_L = X_L \oplus P_i$

$X_R = \mathrm{F}\ (X_L) \oplus X_R$

Exchange X_L and X_R

When the sixteenth round completed, then exchange X_L and X_R again to undo the last exchange.

Then, $X_R = X_R \oplus P_{15}$ and $X_L = X_L \oplus P_{16}$. In last, recombine X_L and X_R to get the cipher text.

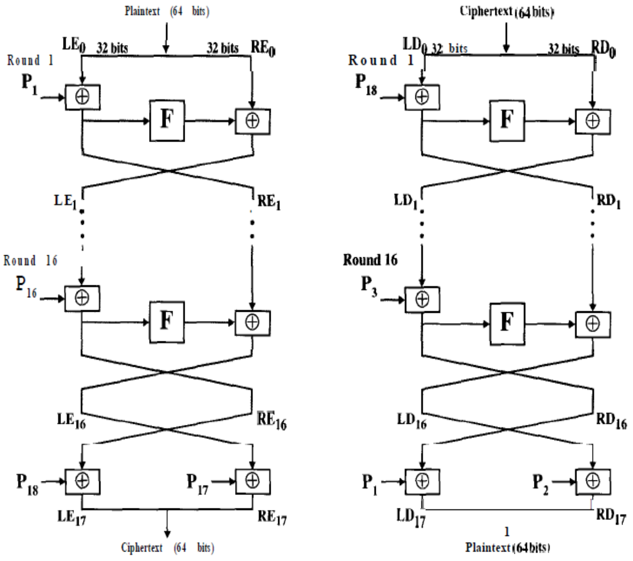

Fig. 1 Structure of Blowfish

In blowfish algorithm 64 bits are used, so the bits are separate into bits and 4 S-Boxes are used. Each S-Box consists of 32 bits. Now the design of the algorithm corresponding 2 S-Boxes joining with XOR for example like same other 2 S-Boxes connected with XOR and then the 2 XOR added and then there get key plain text.

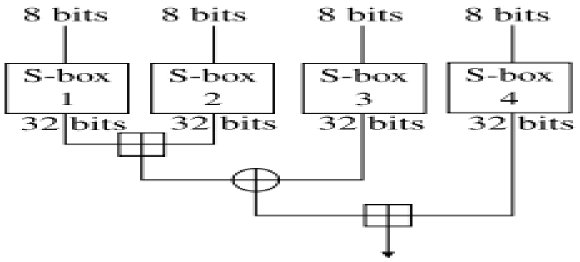

Fig. 2 Blowfish Single Round

Divide X_L into four 8-bit parts: a, b, c, d.

F $[X_L]$ = $((S_1\ [a] + S_2\ [b]\ \mathrm{mod}2^{32}) \oplus S_3\ [c]) + S_4\ [d]\mathrm{mod}2^{32})$

We propose a new security mechanism in VANETs. In proposed scheme we will be use blowfish algorithm for secure transmission of data. Blowfish is identified to be secret-key cipher, which uses a variable number of bits ranging from 32-448 bits and encrypts the data 16 times to make it impossible for an eavesdropper to decrypt it. No attack has been possible to breakdown the blowfish encryption. HECC will be used for key generation and key exchange. In our scheme, security is based on Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP). Eavesdropper cannot hack or destroy HECDLP easily because it is hard and complex.

1.1 General model for VANET

General model for the VANET consists of three different communication which are as follows. General model of VANET is shown in fig.3.

a) Vehicle-to-Vehicle (V2V) Communication

In V2V communication, the vehicles connect with each other's through On Board Unit (OBU) and Application Unit (AU) works behind OBU. V2V communication can provide a data conversation policy for the drivers to share information and send warning messages, i.e. to develop driver support. In V2V Communication there is pure wireless communication between vehicles.

b) Vehicle-to-Road Side Unit (V2R) Communication

In V2R Communication is between mobile nodes and infrastructure unit RSU. V2R communication allows real-time traffic or weather information for drivers and provides an environmental detecting and observing. RSU to trusted authority communication is done through wired media.

c) Vehicle-to-Trusted Authority Communication

In V2T communication vehicles can communicate through wireless broadband devices for example Wi-Fi 3G/4G. As the broadband cloud can contain more traffic information and monitoring data as well as information services, this type of transmission is suitable for active driver assist and vehicle chasing.

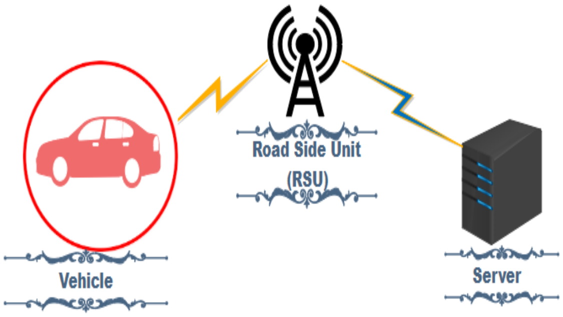

Fig. 3 General Model for VANET

1.2 Applications of VANET

Applications of VANETs are divided into three major groups: i.e. safety oriented applications, convenience oriented applications and commercial oriented applications.

a. Safety Oriented Applications

Safety oriented applications observe the nearby road, surface of the road, upcoming vehicles and road turns etc. They can take control of the vehicle in case of dangerous situations, automatic braking or send warning messages to the drivers. The road safety oriented applications can be categorized as:

Real-Time Traffic: In real time traffic, data can be deposited at the RSU and can be available to the vehicles every time and anywhere required. They plays an important role in solving the problems for example traffic jams, avoid congestions and accidents.

Intersection Damage Notice: The intersection damage notice application informs the drivers when they are going to pass away from a red light. It is probable to attain this application through assigning a RSU with a traffic light controller, therefore RSU broadcast traffic light information. The vehicles which obtains these information can inform the drivers about the existence of a red light to evade accidents before time.

Cooperative Message Transmission: Slow or stopped vehicle motivation exchange messages and cooperate to help other vehicles. However consistency and invisibility would be of main anxiety, it could mechanize things such as emergency braking to evade possible accidents. Also, emergency electronic brake light could be other application.

Post-Crash Warning: Vehicles elaborate in an accident would broadcast warning messages about the position to irregular vehicles, thus it can takings decision with time in addition to highway patrol for drag away maintenance.

Road Threat Control Warning: Vehicle alerting other vehicle about road consuming an information about road feature warning due to sudden downhill, road turn etc.

Electronic Emergency Brakes: This application conducts time-critical emergency messages to vehicles in roads. The electronic emergency brakes application inform the driver that a previous vehicle achieved an unexpected braking. This is suitable that the observation of the braking vehicle is blocked by another vehicles. Braking aggressively, generates a message, which is send in broadcast to inform another vehicles about the dangerous condition.

Compliant Collision Notice: Warns two drivers theoretically about road crash, therefore they may repair their ways.

Traffic Observance: The cameras can be connected at the RSU which can work as input and act like the newest device in small or zero tolerance operation against motivating crimes.

Probe Data Collection: This applications collects data about the vehicle, containing position, encapsulates the data gathered and delivers data in a snapshot to the RSU.

b. Convenience Oriented Applications

Convenience oriented application protect driver's money, save time and increase the competence of the roads. Convenience application mostly compacts traffic management with an objective to improve traffic competence by increasing the amount of accessibility for drivers. The convenience applications can be categorized as:

Route Alterations: Route and tour arrangement may be complete in situation of road blockings.

Electronic Toll Payment: A vehicle creates unicast transmission with a toll point RSU then wages the toll without stopping. Payment of the toll can be done electronically from a toll payment point. A toll payment point is capable to deliver the OBU of the vehicle. OBUs work through GPS and the on-board techograph. Toll application is helpful to both drivers and toll operators.

Parking Accessibility: Vehicles request to a RSU for a list of available parking places, and RSU sends a list to the vehicle.

Active Calculation: It provides the imminent landscape of the road that is predictable to improve fuel usage via altering the travelling speed formerly starting an origin. Moreover, the driver is also supported.

c. Commercial Oriented Applications

Commercial applications facilities the driver as entertaining and web access, streaming audio and video. This type of application works to make the travelling more easy and useful such as, through the internet connection. The commercial applications can be categorized as:

Remote Vehicle Diagnostics: This supports in transferring of personalized vehicle backgrounds or uploading of vehicle diagnostics from an organization. The driver can start a wireless communication with the supplier in order to upload the vehicle diagnostics data to identify possible complications.

Internet Access: Vehicles can access internet through RSU, if RSU is occupied like a router. Hotels and other industries can use a RSU to send publicity information to the drivers of the vehicles, which are in their connection range.

Digital Map Transferring: Map of different areas can be transferred by the drivers as per the requirement before traveling to a new region for travel direction. Similarly, content map database download acts like a gateway for attainment valuable data from home stations or mobile hot spots to download maps and multimedia contents.

Real Time Video Communication: Desire movie experience is not restricted to the controls of the household and the driver can examine real time videos.

Value-Added Announcement: It is specifically for the service suppliers, who need to invite consumers to their stocks. Messages like petrol pumps, highways restaurants to declare their facilities to the drivers within connection range. This application can be accessible even in the nonappearance of the internet connection.

1.3 Security Challenges for VANET

Security is a main problem for all network especially for VANET. When a vehicle share an information to another vehicle, some security challenges are needed which are as follows:

Integrity: The information exchange among the source and the destination must be allowed from the modification attacks. So, information may be reliable.

Authentication: The communication among vehicles in which source and destination information, VANET must authenticate all of them. This procedure contains the ID of the source individuality and the validity of the source to use the setup.

Availability: Availability is distinct as the component of the VANET system, which must be doable and presented while required. A fast reaction interval similarly must appropriate for some requests.

Non-repudiation: This guarantees that the source of information cannot be contradicting that it has transfer the information.

Privacy: Privacy is an important requirements for VANET. Privacy need guarantee that the individuality of the drivers and the position of the vehicles are not being unprotected.

1.4 Preliminaries

Let q be a prime number, where $q \geq 2^{80}$ and Fq finite field of order q. Hyper elliptic curve $C(Fq)$ over finite field be define the equation (i)

$$\mathrm{C{:}\ y2 + h(x)y = f(x)\ mode\ q} \quad \text{(i)}$$

Where $h(x) \in F[x]$ is a polynomial and degree $h(x) \leq g$ and $f(x) \in F[x]$ is a monic polynomial and degree of $f(x) \leq 2g + 1$ points on elliptic curve.

1.4.1 Types of Genus Curve

There are three types of HECC genus curve, genus 2, genus 3 and genus 4.

Genus g=2

$$\mathrm{y2 = x5 + a_3\,x3 + a_2x2 + a_1x + a_0} \qquad \text{(ii)}$$

Genus g=3

$$\mathrm{y2 = x7 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0} \quad \text{(iii)}$$

Genus g= 4

$$\mathrm{y2 = x9 + a_7x7 + a_6x6 + a_5x5 + a_4x4 + a_3x3 + a_2x2 + a_1x + a_0} \qquad \text{(iv)}$$

2. Releated Work

In scheme [3] authors proposed a novel technique based on ECC along with pairing for secure dissemination of data between vehicles and RSU. This scheme is still suffered from security weakness like impersonation attack, Dos attack and DDos attacks. In this scheme only checked the node authenticity while ignored the important security parameter of data authenticity.

In [4], author discussed VANET characteristics, VANET security challenges and constraints. They described different types of attacker i.e. active and passive attacker, malicious and rational attacker, insider and outsider attacker, area attacker, timing attacker and communication attacker. They described security requirement as services i.e. authentication, availability, confidentiality, integrity, non-repudiation, privacy and anonymity and traceability. They proposed different types of VANET attacks and their impact on network. The important attacks which they described are: Brute force attack, Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, node impersonation attack, pranksters, eavesdropping, Global Positioning System (GPS) Spoofing and application attack on safety and non-safety messages.

In [5], author defined only Sybil attack on VANET. In this paper author discussed the fuzzy detection tool against sybil attack. Sybil attack creates when an attacker uses large number of false name, instead of his real ID and affect the modest users by using false name.

In [6], author proposed different steps, first step is located topology of VANET for testing. Second step is located validation of vehicle. In validation first step is to be implemented basic Elliptic Curve Cryptography (ECC) algorithm for validation then accomplished difference in ECC by Adaptive Elliptic Curve Cryptography (AECC) and Enhanced Elliptic Curve Cryptography (EECC) algorithms. In AECC, the key size is adaptive for example different sizes of keys are created during the key generation setup. Three choices are indicated for key sizes: small, large, and medium. In EECC, added an extra constraint during the communication of information from, the vehicle to the RSU for key generation. Third step provided malicious node recognition whereas validation and last step is to be precedence based message forwarding.

In [7], author presented comparison between MANETs and VANETs. They proposed comparative analysis between MANETs and VANET Networks and discussed VANET security requirements. They also described the several types of attacks i.e. location trailing, Denial of Service (DoS) attack, timing attack, sybil attack, replay attack, routing attack, eavesdropping and fake information and also analyzed relative enquiry of security algorithms for VANETs.

In [8], author proposed background information of VANETs and discussed threats, challenges, and requirements in VANETs. In threat section they discussed different types i.e. hardware tampering, bogus information, impersonation attack, Denial of Service (DoS) attack, message suspension and eavesdropping. In requirements section they proposed different schemes i.e. integrated messages as well as efficiently authenticated sources, confidentiality and nonrepudiation, availability and scalability. They proposed algorithms of Digital Signature. In Digital Signature, they discussed different asymmetric cryptography i.e. RSA, ECC (Elliptic Curve Cryptography) and ECDSA (Elliptic Curve Digital Signature Algorithm).

In [9], author presented routing attacks i.e. black hole attack and gray hole attack. They discussed many attackers in VANET i.e. passive attackers, active attackers, insider attackers, outsider attackers, malicious attackers, rational attackers and local attackers. They evaluated comparison between black hole attack and gray hole attack.

In [10], author proposed an integrated multi-level security model and provided the flexibility against malicious attack and purposed to reduce instances of road accidents, as well as to comfort traffic congestions. They described different components of intergraded multi-level of security in VANET. In level one they discussed level of attackers, malicious attackers and behavior of attackers. In level two they defined trusted level and Trust Platform Module (TPM). In level three they defined chain of trust. They also described different Trust Levels and Chain of Trust (CoT).

In [11], author discussed VANET architecture i.e. modules performing communications, modes of communication. They proposed different attacks on the different layers which are attacks at the application layer i.e. message tampering, GPS spoofing attack, malware attack, repudiation and location tracking. They proposed attacks targeting network and transport layer functionalities that are sybil attack, black hole attack, gray hole attack, worm hole attack and impersonation attack. They also discussed attacks on PHYSICAL and MAC layers, these are spamming, DoS attack and DDoS attack.

In [12], author discussed VANET characteristics which are frequent disconnected network, rapid topology changes, battery power and storage capacity, communication environment, mobility modelling and in mobility modeling section they discussed type of the attackers i.e. vandal, hacker, malicious hacker and Insider vs. Outsider and also described capabilities of attackers i.e. technical, resources and coverage area and also proposed types of attacks. They discussed different Network challenges in VANET i.e. Wireless Access Technology, Spectrum Issues.

In [13], author discussed a secure protocol of the VANET for the roadside communication. They also provided the new way of encryption and decryption procedure to improve the communication between vehicle and RSU. They discussed technical challenges in security of VANET i.e. network management, congestion and collision control, environmental impact, MAC design and security. They proposed procedure for creating the key which are key generation procedure, encryption procedure and decryption procedure.

In [14], author proposed an efficient location-based restricted privacy-preserving authentication structure instead of bilinear pairing and tamper-proof devices. They described a CPPA system which is used in VANETs, without using any special devices i.e. TPD. They also proposed a structure which is generated on ECC without any composite bilinear pairing operations. They proposed a scheme i.e. ID-based signature is passed out by ECC, required 160-bits key size to encrypt/decrypt the message which is to be transfer among RSU and vehicle. In terms of energy consumption correspondingly this algorithm needs extra power for its calculation of 160-bits encryption key.

In [15], author observed the authentication problems in VANETs. They proposed conservation and repudiation i.e. ACPN for VANETs. In ACPN, they presented the PKC (Public-Key Cryptography) toward the pseudonym generation. The self-produced PKC created pseudonyms arise as an identifiers beside of vehicle IDs for the privacy-preserving verification, but the updation of the pseudonyms depends on vehicle demands. ID-Based Signature (IBS) system and the IBOOS (ID-Based Online/Offline Signature) structures are used, for the verification among the RSUs (road side units) and vehicles, and the verification between vehicles, similarly. They proposed privacy preservation, non-repudiation, verification and other goals of ACPN, which are observed for VANETs. Classic performance estimation had been directed using efficient IBOOS and IBS structures. They proposed an algorithm which used RSA, this system works ECC-based and ID-based offline or online signatures.

In [16], author proposed efficient batch verifier for the IBS structure. They described batch verifier that can deal with random number of signatures like batch. Then, they analyzed computation cost of the proposed batch verifier using existing parameters and associate it with familiar batch verifiers. They also presented a one-round three-party identity-based key agreement procedure for example an application of batch verifier that needs only three pairing operations in verification. They also proposed batch verifier for shim's IBS, Shim's identity-based signature structure remains defined completed asymmetric bilinear pairing.

In [17], author discussed the basics of the proxy signature approach and also described the ECDSA (Elliptic Curve Digital Signature Algorithm).In ECDSA they discussed that a signer of message followed the three steps i.e. key pair generation, signature generation and verification. They described an ID-based proxy signature environment through Elliptic Curve Digital Signature Algorithm for VANETs.

In [18], author proposed a WAVE-based cross-layer system of provisional privacy-preserving authentication for validation and authenticating vehicular security application messages. They described Elliptic Curve Digital Signature Algorithm (ECDSA), which is used in the ID-based signature, where existing location evidence on a vehicle is applied as the identity of the matching vehicle.

In [19], author proposed a safe privacy-preserving verification that works the usage of aliases for nameless message. They described digital signature structure and combined verification system that are used for vehicular communications, and the ID-based signature system is used for V2R communication. They used password secure OBU, which is one of the procedures that is proposed for the exact attention of less overhead in preserving the keys.

In [20], author proposed a Proxy Based Authentication Scheme (PBAS) using distributed computation. In PBAS, proxy vehicles are used to verify several messages with an authentication function at that time, therefore RSU can freely authenticate the outputs assumed by every alternative vehicles inside its range. They designed further key cooperation structure for transferring complex messages.

In [21], author proposed different applications of VANET i.e. life-critical safety applications and safety warning applications. They discussed different types of attacks for example malicious attack, DoS attack and sybil attack. They also discussed security requirement in VANET i.e. authentication and location detection, preserving privacy and anonymization, active position detection and so on. They described problem of mobility, volatility, network scalability and bootstrap and also discussed VANET Properties supporting security such as high processing power and adequate power supply and Central Registration.

3. Proposed Scheme

In propose scheme we will use blowfish algorithm for encryption/decryption of data, which is symmetric encryption algorithm and HECC for key generation and key exchange, HECC is an asymmetric encryption algorithm. Blowfish algorithm takings a key length from 32 bits to 448 bits for secure data. HECC is more complex when it use Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP). Eavesdropper cannot hack or destroy HECDLP easily.

Table 1: Notation Table

Symbol	Descriptions
H	Hash function
RSU	Road Side Unit
V	Vehicle
X_n	Random number
ID_v	Identification ID for vehicle
Sr	Server
Pb_{sr}	Public key of server
Pr_{sr}	Private key of server
P_{bv}	Public key of vehicle
P_{rv}	Private key of vehicle
C	Cipher text
$\perp$	Rejection

There are four phases of propose scheme.

- Initialization of resources
- Data encryption/decryption
- Key generation and exchange
- Key updating

A. *Initialization of Resources*

Initially public and private keys are loaded on TA/Server. In vehicles its own public and private keys along with public keys of RSU and TA are loaded. All public keys of vehicles and RSU are loaded on TA for secure communication i.e. data encryption.

B. *Data Encryption/ Decryption*

In this phase we used blowfish for encryption and decryption of data. Blowfish is much faster than AES and DES. Blowfish is symmetric algorithm. Vehicle apply hash function to achieve confidentiality and integrity. Vehicle using blowfish algorithm to encrypt the data. Vehicle send encrypted data toward server through RSU. Server decrypt the data and obtain the message and hash value. Server apply hash function to check the integrity of the message. If $H\dot{v}$=Hv its mean data not change during transmission. If $H\dot{v}$≠Hv its mean data change during transmission.

```
Algorithm 1: Encryption
For each vehicle V Ɛ area
1. Sense data of area Ad
2. Calculate hash value Hv=Hash(Ad)
3. Calculate Cd=ER-GK(Ad, Hv)
4. Disseminate Cd to server through RSU

End
```

```
Algorithm 2: Decryption
For each vehicle decrypt data Cd Ɛ area
    1. Ad, Hv=DRGK(Cd)
    2. Calculate $H\dot{v}$=hash(Ad)
    3. Accepted if calculate $H\dot{v}$=Hv data of some area
       otherwise

End
```

C. *Key Generation and Exchange*

In this phase we used HECC for secure key generation and exchange. HECC is an asymmetric algorithm. In this phase server generate session key for secure communication.

```
Algorithm 3: Key Generation and Exchange
Session key generate and exchange 1
    1. Vehicle ($P_{bv}$, $P_{rv}$, $Pb_{sr}$,$ID_v$)
    2. Generate $X_n$Ɛ X {0,1,2,……,n}
    3. H=Hash ($X_n$ ‖ $ID_v$ ‖ Nonce)
    4. C=E $Pb_{sr}$ ($X_n$ ‖ $ID_v$ ‖ Nonce ‖ H)
    5. Communicate cipher text C to server through
       RSU
    6. Server Decrypt ($Pb_{sr}$, $Pr_{sr}$, $P_{rv}$)
    7. $X_n$ ‖ $ID_v$ ‖ Nonce ‖ H)= D $P_{rv}$ (c)
    8. Calculate $\dot{H}$=hash ($X_n$ ‖ $ID_v$ ‖ Nonce)
    9. Accepted if $\dot{H}$=H
    10. Otherwise⊥

Server authentication the vehicle
    11. Vehicle authentication ($ID_v$, Nonce)
    12. Compare received $ID_v$ with stored nonce number
    13. If match correct
    14. Than vehicle allowed
    15. Else vehicle not allowed
    16. Key generation and Encryption/decryption
            a. ($X_{m1}$ ,$X_{m2}$ ,$X_{m3}$ , … … … … ,$X_{mn}$ )
    17. $v_i, v_j$Ɛ ($X_{m1}$ ,$X_{m2}$ ,$X_{m3}$ , … … … … ,$X_{mn}$ )
    18. Calculate key by using randomly selected of
        two numbers
                i. GK= $Xm_i \oplus Xm_j$
    19. Using HECC Ɛ $Pb_{sr}$ (GK)
    20. Encryption secrete key (GK) second encrypted
        key to server
    21. GK=D $Pr_{sr}$ (GK)

        Secrete key=GK
```

D. *Key Updating*

In key updating phase the key will be update after a particular time interval. This updation will be provide forward secrecy and backward secrecy.

```
Algorithm 4: Key Updating
1. Vehicle calculate secrete key RGK
2. Randomly select two numbers i.e. $Xn_1$ , $Xn_2$
3. Then calculate secrete key RGK=$Xm_i \oplus Xm_j$
4. Now coming session secrete key (RGK) will be
   used for next and previous session.
```

4. Performance Analysis

In security analysis our scheme provides authentication, confidentiality and integrity. Performance analysis based on communication cost and computational cost.

The HECC for genus 2, genus 3 and genus 4 are implemented in MATLAB. The equation 2, 3 and 4 are executed in MATLAB.

Table.2 and table.3 show genus 2, 3 and 4 computational cost for prime 40 and 50. Table.4 describe the comparison of DES, 3DES, AES and Blowfish algorithm.

Table 2: Comparison Of Genus 2 To 3 Value For Length Prime 40

	Process time (ms)		
Process	**Genus 2**	**Genus 3**	**Genus 4**
Key generation	2284	3451	7806
Encryption	3222	5319	8113
Decryption	3417	6370	10330

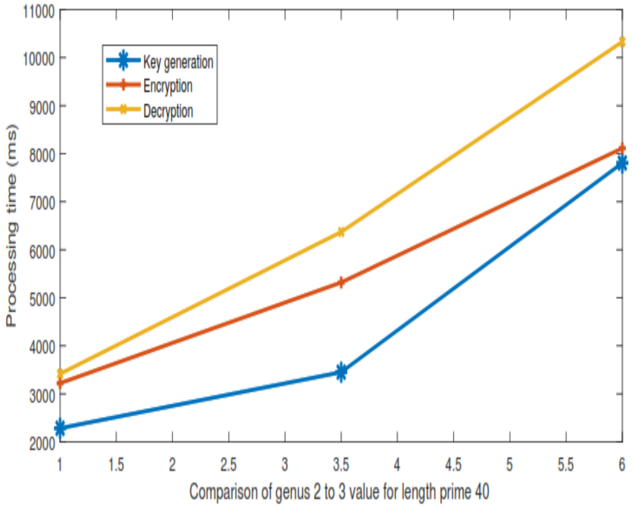

Fig. 4 Comparison of genus2 to 3 value for length prime 40

Table 3: Comparison Of Genus 2 To 3 Value For Length Prime 50

Process	Process time (ms) Genus 2	Genus 3	Genus 4
Key generation	6825	7827	8815
Encryption	3222	6304	8113
Decryption	3417	7670	10330

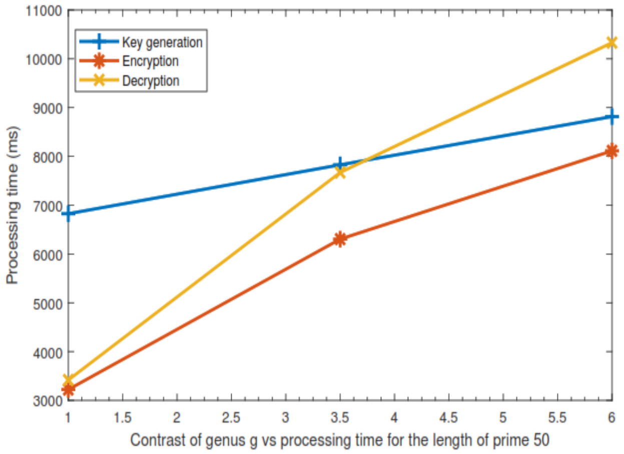

Fig. 5 Contrast of genus g vs. processing time for length prime 50

Table 4: Comparison Of Aes, Des, Triple Des And Blowfish Algorithm

Process	Symmetric Encryption Algorithms AES	DES	3DES	Blowfish
Block Size	128 bit	64 bit	64 bit	64 bit
Key Size	128,192, 256 bit	56 bit	168 bit	32-448 bit
Rounds	10,12,14	16	48	16

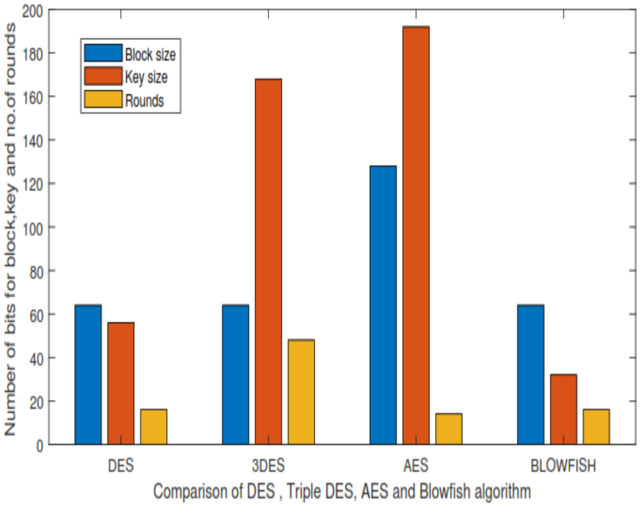

Fig. 6 Comparison of DES, Triple DES, AES and Blowfish algorithm

5. Communication Cost

In fig. (7) we shown the communication cost compression of our proposed scheme and other existing schemes [1,3]. Our proposed hybrid scheme is efficient as compare to other schemes in term of communication cost because we used HECC only for secure key exchange and for encryption/decryption we used blowfish algorithm that make our scheme fast and secure. In exiting scheme [1] HECC used both for key exchange and for secure data transmission among vehicles and RSU while in [3] ECC pairing based scheme used to protect data from adversaries.

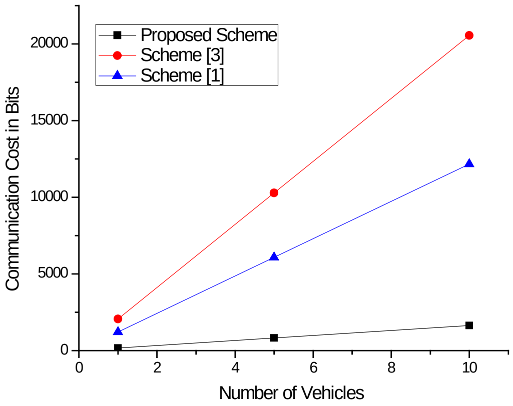

Fig. 7 Communication cost compression

5.1 Computation Cost

To improve the Quality of Service (QoS) in intelligent transportation system vehicles need to quickly computes the important information with less processing cost and then securely exchange with concerned vehicle or RSU for further decision making. We calculate the computational cost compression based on major operations i.e. encryption, decryption, hashing, exponentiation, multiplication, addition and division. In scheme [1] single major operation HECDM consumes 2.2 ms while in scheme [3] one ECPM consume 4.24 ms. In following fig. (8) we shown that the computational cost of our proposed hybrid scheme is less as compared to other existing schemes [1,3].

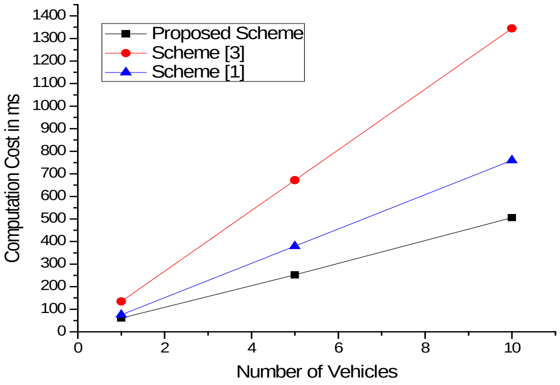

Fig 8. Computational cost comparison

6. Conclusion

Now-a-days VANET security is a hot research topic for researchers. Many accidents occur due to less security in VANET system. For this purpose, we used a new security mechanism for VANET. In this paper, we used a hybrid approach that contains blowfish algorithm and HECC. Blowfish algorithm is used for encryption/decryption of data and HECC is use for secure key exchange. Blowfish is symmetric algorithm and HECC is an asymmetric algorithm. In this paper, we discussed general model for VANET and also discussed different applications of VANET. In this paper, we discussed four phases in proposed scheme i.e. initialization of resources, data encryption/decryption, key generation and exchange and key updating. In performance analysis shown that Our proposed scheme is efficient in term of cost as compared to other two exiting schemes [1,3] and improve the overall security of the VANET.

References

[1] Yadav, K. A. and P. Vijayakumar (2018). Hyperelliptic Curve Cryptography-Based Lightweight Privacy-Aware Secure Authentication Scheme for Vehicular Ad Hoc Network. Intelligent Embedded Systems, Springer: 83-90.

[2] Manku, S. and K. Vasanth (2015). "Blowfish encryption algorithm for information security." ARPN Journal of Engineering and Applied Sciences 10(10): 4717-4719.

[3] K. Iswarya, K. Haridas (2016). "Analysis of Efficient Security Depends on Pairing Based ECC in VANET. " International Journal of Advanced Research in Computer and Communication Engineering.

[4] Upadhyaya, A. N. and J. Shah "Black hole Attack Prevention in VANET."

[5] Bojnord, A. S. and H. S. Bojnord (2017). "A Secure Model for Prevention of Sybil Attack in Vehicular Ad Hoc Networks." International Journal of Computer Science and Network Security (IJCSNS) 17(1): 30.

[6] Godse, S. P., P. N. Mahalle, et al. (2017). "Rising Issues in VANET Communication and Security: A State of Art Survey." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 8(9): 245-252.

[7] Kumar, A. and M. Bansal "A Review on VANET Security Attacks and Their Countermeasure."

[8] Qu, F., Z. Wu, et al. (2015). "A security and privacy review of VANETs." IEEE Transactions on Intelligent Transportation Systems 16(6): 2985-2996.

[9] Rathod, A. and S. Patel (2017). "A SURVEY ON BLACK HOLE & GRAY HOLE ATTACKS DETECTION SCHEME FOR VEHICULAR AD-HOC NETWORK."

[10] Sumra, I. A., P. Sellappan, et al. (2017). "An Integrated Multi-level Security Model for Malicious Attacks Resiliency in Vehicular Ad hoc Network (VANET)."

[11] Nanda, P., N. Malik, et al. (2017). An Overview of Security Challenges in Vehicular Ad-Hoc Networks. 16th International Conference on Information Technology (ICIT).

[12] Al Junaid, M. A. H., A. Syed, et al. (2018). Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. MATEC Web of Conferences, EDP Sciences.

[13] Qazi, F., F. H. Khan, et al. (2017). "Enhancing the Security of Vehicle to Road Side Unit (RSU) Communication with Key Generation and Advanced Encryption Procedure in

Vehicular Ad-Hoc Network (VANET)." Indian Journal of Science and Technology 10(36).

[14] Wu, L., J. Fan, et al. (2017). "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks." International Journal of Distributed Sensor Networks 13(3): 1550147717700899.

[15] Li, J., H. Lu, et al. (2015). "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs." IEEE Transactions on Parallel and Distributed Systems 26(4): 938-948.

[16] Hwang, J. Y., D. H. Choi, et al. (2015). "New efficient batch verification for an identity-based signature scheme." Security and Communication Networks 8(15): 2524-2535.

[17] Biswas, S., J. Misic, et al. (2011). ID-based safety message authentication for security and trust in vehicular networks. Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference On, IEEE.

[18] Biswas, S. and J. Mišić (2013). "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets." IEEE Transactions on Vehicular Technology 62(5): 2182-2192.

[19] Malhi, A. and S. Batra (2016). "Privacy-preserving authentication framework using bloom filter for secure vehicular communications." International Journal of Information Security 15(4): 433-453.

[20] Kudlikar, G. H. and U. Nagaraj (2015). "A Survey on Various Security Schemes in Vehicular Ad hoc Network."

[21] Al-Kahtani, M. S. (2012). Survey on security attacks in Vehicular Ad hoc Networks..(VANETs). Signal Processing and Communication Systems (ICSPCS), 2012 6th International.Conference on, IEEE.

Safia Mushtaq was born on May 28, 1993 in Mansehra, Khyber Pakhtunkhwa (KPK), Pakistan. She received the MCS degree from Hazara University Mansehra. She is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. She is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. Her research interest includes Information Security and Cryptography.
(E-mail: safiamushtaq101@gmail.com)

Dr. Noor Ul Amin is Head Department of Telecommunication at Hazara University Mansehra. He completed his MSc in Computer Science at University of Peshawar in 1996 and his MS and PhD in Computer Sciences at International Islamic University Islamabad, Hazara University Mansehra subsequently. He has recently completed R & D project sponsored by Ministry of Science and Technology, Pakistan. He has been the session chair in the IEEE and Springer conferences. His research interests include Information Security, Wireless Sensor Networks, Steganography and Information-Centric Networking. He has authored more than 80 peer-reviewed journals articles and conference proceedings.
(E-mail: namin@hu.edu.pk)

Mr. Jawaid Iqbal received the BS (Computer Science) degree from Institute of Business and Management Sciences (IBMS), Agriculture University Peshawar in 2010. He obtained the MS (Computer Science) degree with grade very good with honor from Department of Information Technology, Hazara University. Mansehra, K-P, Pakistan. He is currently PhD Scholar (Computer Science) at Department of Information Technology, Hazara University Mansehra, Pakistan. He is currently Lecturer in Department of information technology, Hazara University Mansehra Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2012 up to till date. He believe in quality research in the area of Cryptography, Information and Networks Security. He is currently active in Elliptic/Hyper Elliptic Curve Cryptography, Signcryption, Sensor Networks, Smart Grid and VANT Security. PhD thesis focused on secure communication of sensitive information in Wireless Body Area Networks (WBANs).
(E-mail: jawaid5825@gmail.com)

Chand Bibi obtained the MCS degree from Hazara University Mansehra. She is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. She is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. Her research interest includes Information Security and Cryptography.
(E-mail: chandawan551@gmail.com)

Yousra Saeed obtained the MCS degree from Hazara University Mansehra. She is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. She is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. Her research interest includes Information Security and Cryptography.
(E-mail: yousrakhanswati911@gmail.com)

Irshad Ullah received the BS (Hons) in Computer Science degree from Institute of Information Technology (IIT), Kohat University of Science and Technology (KUST), Pakistan in 2016. He is currently enrolled in MS (Computer Science) at Hazara University Mansehra, Pakistan. He is the Team Member of Smart Cryptography and Networks Research Group in the Department of Information Technology, Hazara University Mansehra from 2017 up to till date. His research interest includes secure communication in Wireless Sensor Networks, Vehicular ad hoc networks (VANETs) and Smart Grid.
(E-mail: irshadullah136@gmail.com)