IJRSET APRIL 2017 Volume 4, Issue 4 Pages: 47-60

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

QFA-ACPN: A NOVEL QUATERNIONS FIREFLY ALGORITHM BASED AUTHENTICATION WITH PRESERVATION AND REPUDIATION FRAMEWORK FOR VANETS

[1] M. RAJESHKUMAR, [2] KARTHIKA. S, [3] M. THARANIDEVI
[1, 2, 3] Assistant Professor,
[1, 2, 3] Department of Computer Applications,
[1, 2, 3] AJK College of Arts Science,

ABSTRACT: A Vehicular Ad Hoc Network (VANET) is a network with the purpose of allows real-time communication among vehicles and road-side units. VANET is a facilitating technology designed for Intelligent Transportation Systems (ITSs). Several number of research work have been in the recent works regarding to the security issue in VANETs, by using symmetric or asymmetric key security methods. Both of these methods symmetric based key security methods are focused rather than the asymmetric key security for VANETs in message authentication. A perfect VANET must have a mechanism in the direction of authenticate vehicles by means of privacy preservation at the same time as maintaining message non-repudiation. In this paper work introduce and develops a novel Quaternions Firefly Algorithm (QFA) based Authentication Framework by means of Preservation and Repudiation (QFA-ACPN) designed for VANETs via the use of IBC method for verification and the pseudonym-based mechanism designed for conditional privacy preservation and non-repudiation in Urban Vehicular Communications (UVC). The major advantages of QFA-ACPN are its reusability. Moreover the solution is extended straightly from PKC, Intrusion Detection based Signature (IBS) and ID-based Online/Offline Signature (IBOOS) schemes, QFA-ACPN have been also utilized by means of new schemes designed for safety and performance improvements. The proposed QFA-ACPN present the conditional vehicle secrecy designed for privacy preservation by means of traceability designed for the non-repudiation, in case with the purpose of malicious vehicles exploitation anonymous authentication techniques in the direction of achieve malicious attacks. In QFA-ACPN, initiate the Public-Key Cryptography (PKC) in the direction of the pseudonym generation, which make sure a legitimate third party in the direction of attain non-repudiation of vehicles by means of finding their real IDs. QFA-ACPN demonstrated that the achievability of ACPN regarding to the system analysis with their parameters such as verification, privacy protection, non-repudiation, time constraint, accessibility and incorporation. Furthermore, the storage and computation overhead of QFA-ACPN is simulated and experimented via the use of network simulation tool.

Keywords: [Vehicular Ad Hoc Network (VANET), Quaternions Firefly Algorithm (QFA), Urban Vehicular Communications (UVC), Authentication Framework with Preservation and Repudiation (ACPN), Intelligent Transportation Systems (ITSs), Public-Key Cryptography (PKC) and ID-based Online/Offline Signature (IBOOS).]

1. INTRODUCTION

A Vehicular Ad Hoc Network (VANET) is a technology with the purpose of make use of moving vehicles is considered as nodes in a network in the direction of generate a mobile network in the direction of present communication connecting vehicles, close by predetermined Road Side Units (RSUs) and Regional Trusted Authorities (RTAs) [1]. A VANET is well thought-out as a variant structure of a Mobile Ad Hoc Network (MANET). It revolves every participating vehicle interested in a node, and permits vehicles in about 300 meters range in the direction of attach with each other. Different the nodes in MANETs, vehicles are operational with Intelligent Transportation Systems (ITS) which usefully have longer transmission ranges, wide-ranging on-board storage space capacities, and rechargeable basis of energy. On the other hand, the mobility of vehicles is controlled by means of predefined roads, the blockage level in VANETs [2]. As mobile wireless devices and wireless networks have been developed with gradually more important areas in the recent years, the demand designed for the Vehicle-To-Vehicle (V2V) communication and the Vehicle-to-Roadside (V2R) communication enlarge constantly.

VANETs are making use of designed for a wide range of security applications, and non-security applications are collision advice, road direction-finding, transfer information and mobile infotainment. In VANETs, the user verification is a critical safety service designed for access manages in together inter-vehicle and vehicle-roadside statement. Conversely, vehicles have in the direction been protected beginning the misuse of their confidential information and the attacks on their confidentiality, for the moment, are able of being examined from accidents. Particularly, security applications needs a well-built mutual validation, since the majority of the safety related messages might hold life-critical information [3].Consequently in this work, together with the growth of the VANET technology depending on the progressing smart vehicles, and additional undiscovered possible issues on security, are devoted in the direction of solving the problems of validation by means of privacy protection and non-repudiation in VANETs.

Several number of research work have been in the recent works regarding to the security issue in VANETs, by using symmetric or asymmetric key security methods. Both of these methods symmetric based key security methods are focused rather than the asymmetric key security for VANETs in message authentication [4-5]. The major disadvantages of using symmetric key management are with the purpose of vehicles contain in the direction of verify each and every methods via the trust authorities, which is not appropriate for huge-scale vehicular transportation in VANETs. On the other hand the use of asymmetric key based authentication is extensively implemented since of the individual keys second-hand designed for encryption and decryption. The works done related to asymmetric key based security methods have been classified into two major classes such as Public Key Infrastructure (PKI) based validation and the Identity (ID) based authentication.

Some of the PKI based validation methods have been developed and proposed [6-9], the system convenience is at rest not persistent or practicable, since such validation methods needs added communication in the direction of handle the vehicular certificates and the Certificate Revocation Lists (CRLs) with the purpose of might reason heavy communication and communication overheads. Validation methods by means of the ID-based signature (IBS) schemes depending on the ID-based Cryptography (IBC) have been introduced and developed in the direction of reducing communication overhead problem in VANET [10-14], in which the certificate management procedure has been fundamental via the use of digital signature methods. IBS schemes have been developed and applied to validation service designed for VANETs, in which each vehicular individuality is second-hand as a public key designed for signing/verifying

messages in statement. By means of using ID-based Online/Offline Signature (IBOOS) is an optimal solution designed for validation in VANETs, designed for solving the computation and communication overhead problem in IBS process. An IBOOS scheme raises effectiveness of the pairing process by means of sorting out the signing process addicted to both offline phase and an online phase, in which the authentication is relatively much efficient than with the purpose of IBS [15-16].

In this paper work introduce and proposed a new authentication framework by means of make use of the IBS scheme in the V2R communication, and simultaneously by means of the IBOOS scheme in the V2V communication designed for better performance. In IBOOS designed for VANETs, the offline phase is able to be implemented primarily next to RSUs or vehicles, while the online phase is in the direction are present implemented in vehicles for the duration of the V2V communication. In VANETs, frequently vehicles' users mightn't their personal information such as vehicle first name, location, moving routes, and user information in the direction of be exposed, in order in the direction of defend themselves adjacent to several prohibited tracing and/or user profiling. With the purpose of the secrecy of vehicular identities must be maintained designed for the confidentiality protection in VANETs. Attain anonymity by means of using vehicle pseudonyms is an optimal solution designed for the confidentiality protection [17], which confidentially associations a real-world identity (ID) in the direction of the related pseudonyms.

In VANETs, the pseudonym of a vehicle might be created by means of the predefined vehicle itself, even be able to be downloaded beginning a trusted link on or after the RTA from time to time [18-19]. Alternatively, when traffic accidents happen, the vehicle secrecy must exist for the time being retrievable, and the individuality information must be exposed to legal authorities in the direction of create the responsibility of accidents which is named as conditional confidentiality. The non-repudiation examine in VANETs protects a vehicle beginning disagree with preceding actions [20]. For instance, vehicles basis accidents must be consistently identified. Accordingly, the conditional privacy protection by means of non-repudiation service is needed designed for VANETs, aligned with the exploitation of anonymous validation techniques by means of malicious vehicles in the direction of attain malicious goals. The pseudonymous validation used in vehicular communications is able to give the privacy preservation by means of a successful tracing mechanism have been used with the trusted authorities in the direction of disclose the real individuality of malicious vehicles. Even though there exist numerous security methods solving the privacy preservation and non-repudiation problems designed for VANETs [21-22], several methods by means of using anonymous credentials which is different from other methods, which render these issues further significant and further difficult in the direction have been applied to VANETs.

2. LITERATURE REVIEW

In VANETs, one of the major important issues with the purpose of when nodes send false node location information in their beacon messages, which know how to rigorously significant the performance of the VANET. A possible source designed for such false location information is malicious nodes. Consequently the safety in VANETs is depending upon the potentially more difficult task of finding and approved malicious data. VANETs have extraordinary necessities in terms of node mobility and location-reliant applications, which are well, gather by means of geographic routing protocols. The intents of an adversary might range beginning basically disconcerting the proper operation of the system in the direction of interrupting traffic exchanged by means of normal users, go behind by means of a promising variation and retransmission.

In [23] introduces and develop a new wireless location privacy attack correlation attack related to the wireless LAN system, and provided an optimal solution with quiet period in the direction of defeat this attack. They also finds the correlation attack as a threat with the purpose of might be routed by means of using periodical pseudonym keep informed solutions and introduced the new method of a silent period in the direction of conflict correlation attacks however there are some other important issues also there earlier than random address be able to be incorporated addicted to wireless communication protocols that is 802.11. Silent period protocol is the initial step designed for us in the direction of realizes wireless location privacy security by means of random address.

In [24] introduces and develops a new authentication method in the direction of determine services by means of roadside units. In this authentication method, they make use of the network layer routing protocols in the direction of establish whether or not the service provider is accessible. If a route in the direction of the service provider is not obtainable, they introduces and develops in the direction of make use of a backbone network to the Internet, in the direction of discover a route. Proposed a new service discovery method and make use of the existence of roadside units in arrange in the direction of raise the effectiveness of service discovery. The results demonstrate the achievability of this new authentication is designed for service discovery in VANET however here they mightn't focus the security issues related to the service discovery.

Misbehaving nodes [25], which contain in the direction of, exist distinguished and not permitted beginning disrupting network operation, an issue mainly difficult in the direction of address in the life-dangerous VN environment. Existing VANET networks depends majorly on node credential revocation designed for attacker deportation, however the be deficient of an universal communications in VNs may possibly inappropriately interruption the recovery of the majority current and appropriate revocation information; this determination particularly be the case in the early exploitation stages such as extremely unpredictable and large-scale scheme. Attain the revocation they introduce a new methods in the direction of the individuality of the VANET. In the direction of remove the vulnerability window, appropriate in the direction of the latency designed for the authority in the direction of recognize faulty and distribute revocation information, developed a scheme with the purpose of can strongly and proficiently attain their separation, in addition to add in the direction of their eventual revocation however author not converse on each of the individual components of the framework.

In [26] develops a new Anonymous Batch Authenticated and Key Agreement (ABAKA) scheme in the direction of validate multiple requests launch beginning varied vehicles and begin varied session keys designed for varied vehicles simultaneously. In VANETs, the velocity of a vehicle is altered from 10 to 40 m/s (36–144 km/h); consequently, the necessitated designed for proficient validation is predictable. By means of ABAKA, an SP is able to concurrently validate many requests and create varied session keys by means of vehicles. ABAKA regard as not only scalability and safety issues however privacy preservation as well and in the direction of handle by means of the unacceptable request problem, a detection algorithm have been also developed however they also not focus on the information regarding the problems like mobility model and predicable routing, scheming novel schemes in the direction of increase additional effectiveness.

In [27] mostly address problem of mitigating unauthorized tracking of vehicles taking place their broadcast relations, toward enhance user location privacy during VANET as well as suggest a scheme called AMOEBA, which provide position privacy as a result of utilize the group navigation of vehicles. Proposed a scheme, call AMOEBA so as to provide location privacy through mitigating the location tracking of vehicles, as well as protects user privacy through providing vehicles among anonymous way in toward

LBS applications along through he discussed regarding robustness along with liability of the proposed scheme, against active attacks taking place vehicle safety however here author not considered on mobility of vehicles to facilitate will incorporate intersection performance suitable toward traffic signs along with effects of congested streets, combine through map data as well as with communication traffic models.

Lin et al [28] Proposed Group Signature as well as Identity-based Signatures (GSIS) method offer protection along with conditional privacy within VANETs. This method offers attractive security necessities such as authentication, reliability, as well as anonymous user confirmation, vehicle anonymity, along with RSU ID exposure, preclusion of RSU replication, vehicle ID traceability, furthermore effectiveness. GSIS tackle security troubles as a result of taking a dissimilar approach toward secure communication among vehicles and communication among vehicles also RSUs since they encompass different security requirements. Thus, used for V2V communication, group signature is employed as well as messages preserve be securely and anonymously be signed by the senders, whereas road authorities preserve reveal the identities of the senders at what time required. The privacy necessity of V2I is not as sensitive as V2V communication. Thus GSIS choose a signature method by means of ID based cryptography (IBC) toward digitally sign each message sent through RSUs to ensure origin authentication along with this significantly minimizes signature overhead. GSIS exploit the reality that, several strings be able to serves as a valid public key in IBC.

Temporary Anonymous Certified Keys (TACKs) [29] is a method to facilitate offers authentication, confidentiality, short-term link ability, traceability, revocation, as well as efficiency. TACK largely employs grouping signatures toward satisfy its security requirements. The propose of TACKs groups the roads into geographic regions as well as assumes so as to each geographical region there is Regional Authorities (RA) which be capable of serve since a certificate authority. Moreover, federal transportation authority determination exists root of the key hierarchy. This assumption is reasonable as well as it make TACKs appropriate used for easy interoperability. TACK employs grouping signature system proposed during [30]. The idea is so as to each member of have a group user key, a long-term private key, issue by means of a trusted group manager, such as Department of Motor Vehicles (DMV). When vehicle requirements toward get a certificate used for short-lived TACK from its individual RA, it signs request message through its group user key. The short-lived TACK is designed for signing messages. The vehicle periodically broadcasts its certificate, consequently others can verify the signed message it sends. The TACK has a very small life time along with it has toward update when lifetime ends otherwise when vehicle joins a new geographical region. The update of TACK is performing as follows. The vehicle's OBU randomly generate a new TACK public/private key pair as well as uses group user key toward sign TACK public key along with then it sends signed public key toward RA for the region toward certify it group signature on received TACK public key along with checks requestor against revocation list. If the verification is successful, a RA sign a certificate for requester's TACK public key, stores associated values locally for later use along with sends certificate back after some t seconds. The delay is intentionally added since a thwart next to link ability. The main drawback of this approach pointed out during [31] is so as to a vehicle which have been revoke be able toward still maliciously communicate through a valid certificate because revocation during this scheme only prevents node from getting a new certificate.

Fischer et al [32] introduces and develops a new Secure Revocable Anonymous Authenticated Inter-Vehicle (SRAAC) scheme with the intention of intends in the direction of enhance the following security issues of Wireless Access in Vehicular Environment (WAVE) a standard described in IEEE 1609.2 security standard . By the use of weak

encryption in the direction of defend message unlinkability. Addiction on a single certification authority designed for issuing each and every one anonymous certificate might lead in the direction of linkage of certificates and vehicles. High memory and bandwidth consumption are major important issues, since of Certificate Revocation List (CRL) procedure.

3. PROPOSED METHODOLOGIES

In this paper work introduce and develops a novel Quaternions Firefly Algorithm (QFA) based Authentication Framework by means of Preservation and Repudiation (QFA-ACPN) designed for VANETs via the use of IBC method for verification and the pseudonym-based mechanism designed for conditional privacy preservation and non-repudiation in Urban Vehicular Communications (UVC). The major advantages of QFA-ACPN are its reusability. Moreover the solution is extended straightly from PKC, Intrusion Detection based Signature (IBS) and ID-based Online/Offline Signature (IBOOS) schemes, QFA-ACPN have been also utilized by means of new schemes designed for safety and performance improvements. The proposed QFA-ACPN present the conditional vehicle secrecy designed for privacy preservation by means of traceability designed for the non-repudiation, in case with the purpose of malicious vehicles exploitation anonymous authentication techniques in the direction of achieve malicious attacks. In QFA-ACPN, initiate the Public-Key Cryptography (PKC) in the direction of the pseudonym generation, which make sure a legitimate third party in the direction of attain non-repudiation of vehicles by means of finding their real IDs. This PKC schemes determination is useful in the proposed QFA-ACPN authentication framework intended for VANETs. Note with the purpose of the traditional IBS and IBOOS schemes not useful for VANETs. Thus, we adjust the predictable method designed for VANETs by means of allocating functions in the direction of position in a VANET. In this section present the beginning set of the PKC scheme, combination designed for ID-based cryptography, IBS scheme and the IBOOS scheme, correspondingly designed for VANETs. QFA-ACPN demonstrated that the achievability of ACPN regarding to the system analysis with their parameters such as verification, privacy protection, non-repudiation, time constraint, accessibility and incorporation.

Pairing for IBC

ID-based cryptography [33-34] permit the public key of an entity in the direction be derived beginning its public identity data such as name, email address, etc., which keep away from the make use of certificates designed for public key authentication in the traditional PKI. Many of the methods related to the IBC are performed based on the Diffie-Hellman (BDHP) and Elliptic Curve Cryptography (ECC) domain, where the Discrete Logarithm Problem (DLP) designed for combination in groups is needed to be hard. Designed for self-contained, we detail explain the distinctiveness of pairing. Indiscriminately chose two large primes p and q, and let $E=F_p$ designate over a finite field F_p. Represent a q-order subgroup of the additive group of points in E=Fp by means of G_1, and a q-order subgroup of the multiplicative group in the restricted field F.

IBS Scheme for VANETs

IBC based ID-based signature scheme [35] is used in VANETs which includes of four major setup which are described as follows that is setup, key extraction, signature signing and verification:

Setup: The RTA determines a master key s and free parameters param designed for the Private Key Generator (PKG), and provide param in the direction of each and every one vehicles.

Extraction: Depending on an ID string, a vehicle creates a private key sekID connected with the ID by means of the master key s.

Signature signing: Depending on a message M, time stamp t and a signing key u, the sending vehicle creates a signature SIG.

Verification: Depending on the ID, M and SIG, the receiving vehicle outputs "accept" if SIG is suitable designed for confirmation, and outputs "reject" or else.

IBOOS Scheme for VANETs

An ID-based online/offline signature scheme [36] beginning IBC second-hand in VANETs includes of five major steps which are described as follows such as setup, key extraction, offline signing, online signing and verification: Setup: This step is similar like as in IBS scheme. Extraction: The RTA creates a private key sek_{ID} related with the ID by the means of the master key s. Offline signing: Depending on the sek_{ID} and public parameters, the RTA/RSU creates an offline signature $SIG_{offline}$ designed for each vehicle. Online signing: Depending on the offline signature $SIG_{offline}$ and a message M, the sending vehicle creates an online signature SIG_{online} of M. Verification: Depending on the ID, M and SIG_{online}, the receiving vehicle outputs "accept" if SIG_{online} is valid designed for confirmation, and outputs "reject" or else.

4. INITIALIZATION OF PROPOSED SCHEMA

In this paper work introduce and develops a novel Quaternions Firefly Algorithm (QFA) based Authentication Framework by means of Preservation and Repudiation (QFA-ACPN) designed for VANETs via the use of IBC method for verification and the pseudonym-based mechanism designed for conditional privacy preservation and non-repudiation in Urban Vehicular Communications (UVC). The major advantages of QFA-ACPN are its reusability. Moreover the solution is extended straightly from PKC, Intrusion Detection based Signature (IBS) and ID-based Online/Offline Signature (IBOOS) schemes, QFA-ACPN have been also utilized by means of new schemes designed for safety and performance improvements. The proposed QFA-ACPN present the conditional vehicle secrecy designed for privacy preservation by means of traceability designed for the non-repudiation, in case with the purpose of malicious vehicles exploitation anonymous authentication techniques in the direction of achieve malicious attacks. In QFA-ACPN, initiate the Public-Key Cryptography (PKC) in the direction of the pseudonym generation, which make sure a legitimate third party in the direction of attain non-repudiation of vehicles by means of finding their real IDs. In this research work QFA-ACPN based authentication framework is designed for VANETs, let us consider a framework under the UVC structure which includes of information about RTA, limited numbered registered RSUs the length of roadsides, and a huge number of vehicles. An RTA provides in one region, e.g., a city, a country. An ID pool of RSUs in an area is pre-full in every vehicle, in which the number of RSUs is frequently set with the purpose of mightn't alter regularly. The vehicle registration is needed earlier than a vehicle establish off in the direction of knock the road in an area. If the vehicle is recently affected, it is able to be listed in the direction of the RTA on the car dealer by means of a secure network infrastructure. If a vehicle is driven addicted to a new area, it is able to be registered in the direction of the RTA on the entry-exit administration. All the way through the vehicle registration of every vehicle, the RTA registers the vehicle ID and profile designed for validation in the direction of the vehicle. Make use of Figure 1 in the direction of demonstrate the operations of the proposed QFA-ACPN designed for VANETs.

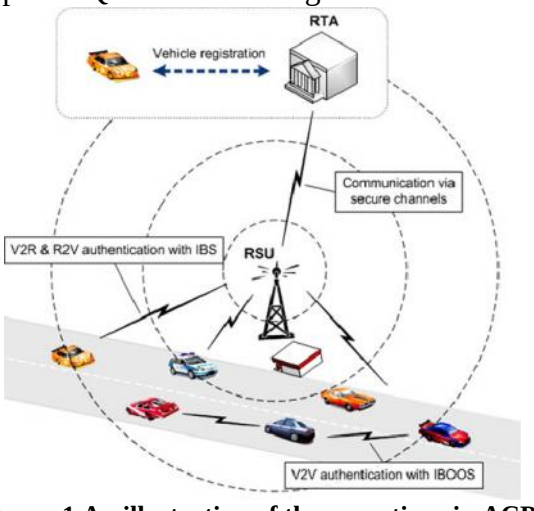

Figure - 1 An illustration of the operations in ACPN for VANET

Pseudonym Generation

In ACPN designed for confidentiality preservation, the PKC depending on the pseudonym of a vehicle is created instead of the real-world ID in the confidentiality process. Since the RTA is occasionally broadcasting the present public key by means of RSUs designed for the PKC in the pseudonym generation, the vehicle is able to use it designed for the PKC-based pseudonym generation, when it requirements in the direction of update its present pseudonym $PS_v \stackrel{def}{=} Time \left|\left|E_{pk}(ID_v)\right|\right| HR|RSU$ where Time, when the pseudonym is created. E_{pkc} (ID_v) is the encrypted value created from the vehicle's real ID, by means of using the present PKC's public key pkc determined from the RSU broadcasts. HR indicates the code name of the vehicle's home area. RSU represents the ID of the present consequent RSU, where the vehicle creates its new pseudonym designed for secure verification and message communication. The proposed ACPN operates adaptively, at whatever time a vehicle needs in the direction of recently authenticates itself to others. Here introduce a new Intrusion Detection System (IDS) designed for DDoS attack detection such as DAN, which categorized into the Network Traffic Analyzer, Traffic Features recognition and Extraction, and Intruder data. DDoS attacks have been categorized into two major types such as vulnerability and flood attacks. Intruder generates this type of vulnerability by means of sending spoofed packets by means of SYN Flag in the direction of the victim which results addicted to lock up. The packet consists of identical source, destination address and the victim machine presumes with the purpose of sending itself, resulting addicted to collide the mechanism.

Quaternions Firefly Algorithm (QFA), Fireflies are insects, the major characteristic of which is their flashing lights with the purpose of be able to be well-liked in the summer sky on night. These fireflies lights contain two basic functions, specifically in the direction of magnetize mating partners and in the direction of notify off possible predators. The flashing lights 'intensity I reduces with distance r increases related in the direction of the term $I \alpha I/r^2$to create the FA. In the direction of evade impulsive convergence in FA algorithm is combined with a quaternion's representation. In arithmetic, quaternions expand complex information.

On the other hand fitness value is computed not only depending on the distance among source to destination node and the p_i be a factor with the purpose of decreases the probability of the success of a_i. The flashing lights 'intensity I reduces with distance r increases related in the direction of the term $I \alpha I/r^2$to create the FA. Here, the light-intensity is proportional in the direction of the fitness function of the problem individual optimized (i.e., $I(f) \propto fit(f)$, where $f = Pr(a_j|m_j)$ denotes optimal solutions are described as follows:

The QFA is performed based on the behavior of FA, where the description of virtual fireflies is moved from a space to a quaternion Mahalanobis distance space. In the Mahalanobis distance, each virtual firefly is denoted as D-dimensional real-values with N nodes vector $N = (n_1, .. n_N)$, where $N_{ij} \in \mathbb{R}^n$, quaternion space as $q_i = \{q_{i0}, .. q_{in}\}$, where $q_{ij} \in \mathbb{H}^n$. Subsequently, the search-process might be directed in the direction of the more promising areas of the investigate-space.

The MWQFA is varied from FA by means of using the quaternion's representation of nodes are applied. Quaternions are formal expressions $q = x_0 + x_1 i + x_2 j + x_3 k$, where x_0, x_1, x_2, x_3 are real values and they comprise the algebra over the real numbers created by means of basic units i, j, k (also the imaginary part) with the purpose of assure Hamilton's equations:

$$= i, k \quad (1)$$

$$= -i, \quad (2)$$

$$k^2 = -1 \quad (3)$$

The quaternions $q \in \mathbb{H}$ defines a 4-dimensional space over the real numbers. By means of this notation, a pair of quaternions is represented as $q_0 = x_0 + x_1 i + x_2 j + x_3 k$ and $q_1 = y_0 + y_1 i + y_2 j + y_3 k$. The quaternion algebra described with the

operations is calculation and subtraction, scalar multiplication, multiplication. In adding together in the direction of pure quaternion algebra, two unary functions are described as follows: qrand() is a quaternion described as follows,

$$\{x_i = N(0,1) \text{ is described as random} \quad for\ i = 0,..3\} \quad (4)$$

where $N(0,1)$ is described as random number computed from Gaussian distribution function with zero mean and standard deviation one. qzero: is a quaternion described as follows

$$(5)$$

The QFA with population of quaternions is initialized in InitQFA() by means of using the qrand() function. The solution $f = Pr(a_j|m_j)$ in the Mahalanobis- distance is determined from i-th quaternions' vector q_i by means of the norm function as described as follows:

$$f_{ij} = ||q_{ij}||, for\ j = 1\ to\ D \quad (6)$$

Determining the Mahalanobis- distance among the nodes in the VANET search-space is expressed with high Packet Delivery Ratio (PDR)

$$r_{ij}^2 = d_{ij}(q_{ij}) = \sqrt{(w_i - w_j)^2} \quad (7)$$

where q_i is the i-th virtual firefly location, and q_j is the j-th virtual firefly location in the search-space. Moving the firefly i in the direction of another more attractive firefly j as described as follows:

$$d_{ij}(q_{ij}) = \sqrt{(w_i - w_j)^2} \quad (8)$$

$$= q_i + \beta_0 e^{-\gamma r_{ij}^2}(q_j - q_i) + \alpha.\varepsilon.Qrand() \quad (9)$$

where r_{ij}^2 represents the distance between two nodes in the quaternion's space in VANET architecture , α is the randomization parameter, ε the scale, and the $Qrand()$ is a quaternion random vector. In this work the fitness value is computed based on the weight values of the nodes to the $fitness_i$ have been assigned to the solution q_{ij} by (10).

$$fitness^i = \begin{cases} \frac{1}{(1 + fit_i.w_i)} & if\ f_i.w_i \geq 0 \\ \frac{1}{(abs(fit_i.w_i))} & if\ f_i.w_i < 0 \end{cases} \quad (10)$$

where fit_i is the probability value of the nodes.

V2R and R2V Authentication

The V2R and R2V validation is performed based on the V2V authentication, which consists of the following steps as most important steps.

Step 1: The RSU is broadcasting its information from time to time, which is second-hand designed for the V2R and R2V validation. Consequently, the vehicles in the transmission range be able to obtain the RSU's information <ID_r; T; p_{kc}; adv; nonce; $SIG_r(ID_r.||T)$, here IDr is the ID of the broadcasting RSU, T is the time stamp designed for the present time interval. pk_c is the public key of PKC, which is second-hand at the time of time interval. The advertisement message adv is the request of V2R verification in the subsequently step and the nonce is for freshness. $SIG_r(ID_r.||T)$, is the IBS designed for R2V validation, which is created from the RSU's ID_r and the time stamp T.

Step 2: A vehicle respond a message in the direction of the related to RSU in either of the subsequent two cases, by means of using IBS designed for V2R authentication: A vehicle wants in the direction of recently create or revise its pseudonym designed for validation and communication in the VANET system. A vehicle receives an original RSU ID from an RSU's broadcast.

Step 3: Following in receipt of the join request message beginning a vehicle, the RSU authenticate the signature, and acknowledge it if the message is valid. The RSU initial inform the pseudonym PS_v in its memory, in addition to reports it in the direction of the RTA. Afterwards, the RSU creates the offline signatures SIGoffline (PS_v) from the pseudonym PS_v designed for the vehicle V_v

V2V Authentication

The V2V validation, which is furthermore named inner-RSU V2V validation, is second-hand designed for safe vehicular communication between vehicles. At the time of the V2V authentication, vehicles make use of the received POI sets designed for authentication and verification. As a sender, the vehicle initially calculates the online signature SIG_{online} begining the offline signature $SIG_{offline}$, by means of using the IBOOS scheme designed for validation. Then, the receiver vehicles are able to make use of the online signature designed for the V2V validation. In case with the purpose of vehicle v is prepared in the direction of validate itself in the direction of other vehicles in its transmission range, it primary calculates the online signature SIG_{online} v ($SIG_{offline}$v (PS_v||t) from the offline signature $SIG_{offline}$ v PS_v and the time stamp t. from the received authentication message in the sender vehicle, the vehicles in the sender's transmission range confirm the online signature by means of the related POI set stored in their memories.

5. SIMULATION RESULTS

In this section simulate the performance and efficiency of QFA-ACPN and ACPN, designed for UVC in VANETs all the way through system examination and evaluation in terms of key generation time, computation overhead by execution time and verification effectiveness.

Storage Requirements

In the proposed QFA-ACPN and ACPN, the storage requirements on RTAs and RSUs are not stringent because these entities are distributed and resource-free in environment in VANETs. It is mostly disturbed by means of the storage cost in vehicles beginning two respects, the information essential designed for cryptographic parameters, and the number of POI sets designed for the V2V verification.

Computation Overhead

This part gives an estimation of efficiency on applying the proposed QFA-ACPN and ACPN designed for VANETs, by means of examine the computation overhead. Focal point by proposing IBS and IBOOS schemes in the direction of ACPN, since the implements PKC schemes used in the pseudonym generation which mightn't affect the effectiveness of verification for the period of communication in VANETs.

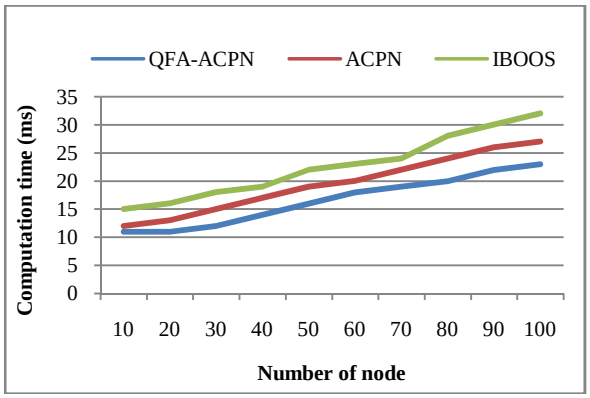

Figure - 2 Computation time vs. number of nodes

Figure 2 illustrates the performance comparison results of computation time with number of sensor nodes between 10 and 100. From the results it concludes that the proposed QFA-ACPN needs lesser computation results of 23 ms for 100 numbers of nodes which is 4 ms, 9 ms lesser when compared to ACPN, and IBOOS methods respectively (shown in Figure 2 and table 1).

	Computation time (ms)		
No. of nodes	QFA-ACPN	ACPN	IBOOS
10	11	12	15
20	11	13	16
30	12	15	18
40	14	17	19
50	16	19	22
60	18	20	23
70	19	22	24
80	20	24	28
90	22	26	30
100	23	27	32

Table - 1 Computation time vs. No. of nodes

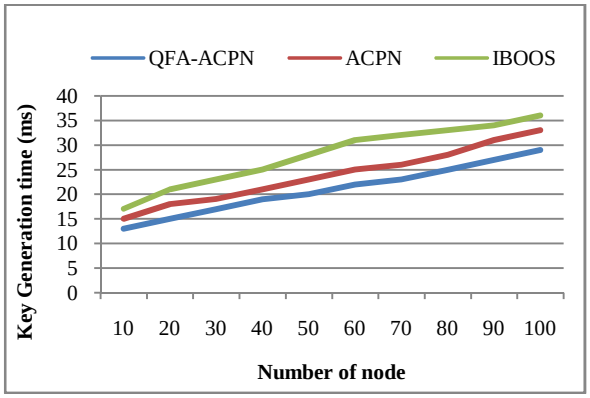

Figure - 3 Key Generation time vs. No. of nodes

Figure 3 illustrate the performance comparison results of key generation time with number of sensor nodes between 10 and 100. From the results it concludes that the proposed QFA-ACPN needs lesser key generation time of 29 ms for 100 numbers of nodes which is 4 ms, 7 ms lesser when compared to ACPN, and IBOOS methods respectively (shown in Figure 3 and table 2).

No. of nodes	Key Generation time (ms)		
	QFA-ACPN	ACPN	IBOOS
10	13	15	17
20	15	18	21
30	17	19	23
40	19	21	25
50	20	23	28
60	22	25	31
70	23	26	32
80	25	28	33
90	27	31	34
100	29	33	36

Table - 2 Key Generation time vs. No. of nodes

Authentication Efficiency

In this part, the effectiveness of mutual verification between vehicles in VANETs is examined through theoretical quantitative calculations designed for UVC. This part gives an estimation of efficiency on applying the proposed QFA-ACPN and ACPN designed for VANETs, by means of examine the Authentication Efficiency. In ACPN, the effectiveness of authentication is evaluated by means of the communication delay between vehicles, in which focus on the computational delay inspired by means of using cryptographic techniques including IBS and IBOOS schemes.

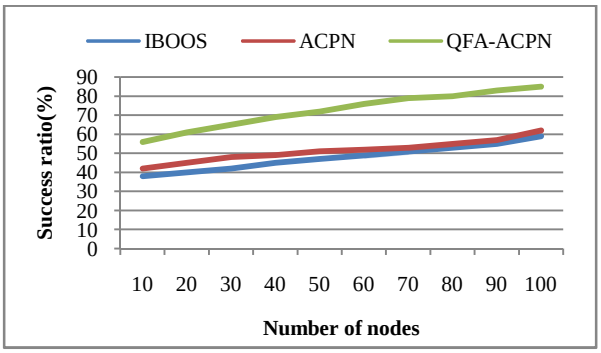

Figure - 4 Authentication Efficiency vs. number of nodes

Figure 4 illustrates the performance comparison results of authentication efficiency with number of sensor nodes between 10 and 100. From the results it concludes that the proposed QFA-ACPN needs lesser computation results of 23 ms for 100 numbers of nodes which is 4 ms, 7 ms, 9 ms higher when compared to ACPN, and IBOOS methods respectively (shown in Figure 4 and table 3).

No. of nodes	Authentication efficiency		
	QFA-ACPN	ACPN	IBOOS
10	56	42	38
20	61	45	40
30	65	48	42
40	69	49	45
50	72	51	47
60	76	52	49
70	79	53	51
80	80	55	53
90	83	57	55
100	85	62	59

Table - 3 Authentication Efficiency vs. No. of nodes

CONCLUSION AND FUTURE WORK

VANETs contain an enormous prospective in the direction of fundamentally enhances safety and driving knowledge along the roads and highways. An Identity management system should contain

precondition with the purpose of should be developed and introduced in the direction of use of VANETs, elsewhere VANETs might be used by means of malicious parties in a way with the purpose of would expose the advantages of their deployment. In work propose a novel Quaternions Firefly Algorithm (QFA) based Authentication Framework with Preservation and Repudiation (QFA-ACPN) designed for VANETs, by means of using the IBC designed for authentication .This methods is proposed with QFA based pseudonym-based mechanism designed for conditional privacy preservation and non-repudiation in Urban Vehicular Communications (UVC). This method QFA-ACPN make use of the Intrusion Detection based Signature (IBS) and ID-based Online/Offline Signature (IBOOS) schemes designed for the verification, the QFA based pseudonym-based mechanism designed for the privacy protection. QFA-ACPN attains the preferred validation, privacy protection, non-repudiation and additional safety objectives designed for UVC in VANETs. An additional important attribute of ACPN is its reusability that has been also is making use of through other new schemes designed for safety and performance improvements. The proposed QFA-ACPN principally efforts in the direction of present validation and privacy preservation by means of non-repudiation in VANETs, and determine the conflicts among them. Simulation results and performance evaluation show with the purpose of the proposed QFA-ACPN is practicable and sufficient to UVC in the VANET environment designed for well-organized privacy-preserving authentication by means of non-repudiation. The simulation results also demonstrate with the purpose of the effectiveness of QFA-ACPN designed for UVC in VANETs all the way through system investigation and theoretical results in terms of storage requirement, computation overhead and authentication efficiency. On the other hand, we have not officially established the security of the confirmation flows. Consequently, a probable future direction is able to be to make use of protocol verification tools in the direction of verify the verification flows. This work is able to be more extensive by means of investigate ways in the direction of optimize the IMS Authentication and Key agreement (IMS-AKA) process in the VANETs architecture.

REFERENCES

[1]. S. Zeadally et al., “Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges,” Telecomm. Systems, vol. 50, no. 4, pp. 217-241, 2012.

[2]. F. Li and Y. Wang, “Routing in Vehicular Ad Hoc Networks: A Survey,” IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12- 22, 2007.

[3]. M. Raya and J. Pierre, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[4]. X. Lin, “TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving,” IEEE Trans. Wireless Comm., vol. 7, no. 12, pp. 4987-4998, 2008.

[5]. A. Studer et al., “Flexible, Extensible, and Efficient VANET Authentication,” J. Comm. and Networks, vol. 11, no. 6, pp. 574-588, 2009.

[6]. “IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE),” U.S. Dept. Transportation, 2009.

[7]. N.-W. Wang, Y.-M. Huang, and W.-M. Chen, “A Novel Secure Communication Scheme in Vehicular Ad Hoc Networks,” Computer Comm., vol. 31, pp. 2827-2837, 2008.

[8]. R. Lu et al., “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,” Proc. IEEE INFOCOM, pp. 1229-1237, 2008.

[9]. Y. Sun et al., “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, 2010.

[10]. P. Kamat, A. Baliga, and W. Trappe, “An Identity-Based Security Framework for VANETs,” Proc. Third Int’l Workshop Vehicular Ad Hoc Networks (VANET), pp. 94-95, 2006.

[11]. Y. Zhang et al., "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 386-399, 2006.
[12]. P. Kamat, A. Baliga, and W. Trappe, "Secure, Pseudonymous, and Auditable Communication in Vehicular Ad Hoc Networks," Security and Comm. Networks, vol. 1, no. 3, pp. 233-244, 2008.
[13]. X. Lin et al., "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007.
[14]. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, 2010.
[15]. S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. CRYPTO: Advances in Cryptology, pp. 263-275, 1990.
[16]. F.R. Yu et al., "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks," IEEE Trans. Network and Service Management, vol. 7, no. 4, pp. 258-267, 2010.
[17]. H. Dok et al., "Privacy Issues of Vehicular Ad-Hoc Networks," Int'l J. Future Generation Comm. and Networking, vol. 3, no. 1, pp. 17-32, 2010.
[18]. M. Gerlach and F. Guttler, "Privacy in VANETs Using Changing Pseudonyms—Ideal and Real," Proc. IEEE Vehicular Technology Conf. (VTC-Spring), pp. 2521-2525, 2007.
[19]. H. Lu, J. Li, and M. Guizani, "A Novel ID-Based Authentication Framework with Adaptive Privacy Preservation for VANETs," Proc. Comm. and Applications Conf. (ComComAp), pp. 345-350, 2012.
[20]. F. Armknecht et al., "Cross-Layer Privacy Enhancement and Non- Repudiation in Vehicular Communication," Proc. ITG-GI Conf. Comm. in Distributed Systems (KiVS), pp. 1-12, 2007.
[21]. J. Choi and S. Jung, "A Security Framework with Strong Non- Repudiation and Privacy in VANETs," Proc. IEEE Sixth Consumer Comm. and Networking Conf. (CCNC), 2009.
[22]. J. Sun, C. Zhang, and Y. Fang, "An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," Proc. IEEE Military Comm. Conf. (MILCOM), pp. 1-7, 2007.
[23]. Leping Huang, Kanta Matsuura, Hiroshi Yamane and Kaoru Sezaki "Enhancing Wireless Location Privacy Using Silent Period" IEEE Communications society/WCNC 2005.
[24]. Brijesh Kadri Mohandas, Amiya Nayak, Kshirasagar Naik and Nishith Goel "ABSRP - A Service Discovery Approach for Vehicular Ad-Hoc Networks" IEEE Asia-Pacific services computing conference, 2008.
[25]. Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels and Jean-pierre Hubaux "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks" IEEE Journal on Selected areas in Communications, Vol 25, No.8, 2007.
[26]. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien "ABAKA:An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, Vol 60, No.1, 2011.
[27]. Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran "AMOEBA: Robust Location Privacy Scheme for VANET" IEEE Journal on Selected Areas in Communications, Vol 25, No.8,2007.
[28]. X. Lin, X. Sun, P.-H. Ho, and X. Shen, GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," Vehicular Technology, IEEE Transactions on, vol. 56, no. 6, pp. 3442-3456, 2007.
[29]. Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. 2009. TACKing together efficient authentication, revocation, and privacy in VANETs. In Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'09). IEEE Press, Piscataway, NJ, USA, 484-492.
[30]. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In:

Proceedings of ACM CCS 2004, pp. 168–177. ACM Press, New York (2004).
[31]. OpenID Foundation, OpenID Foundation http://openid.net/foundation/. 25. L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)," in Proceedings of the 4th Annual Conference on Embedded Security in Cars (escar 2006), is-its, 2006.
[32]. P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06, pp. 94-95, 2006.
[33]. P. Barreto et al., “Efficient Algorithms for Pairing-Based Cryptosystems,” Proc. CRYPTO, pp. 354-369, 2002.
[34]. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” Proc. CRYPTO, pp. 47-53, 1985.
[35]. A. Shamir and Y. Tauman, “Improved Online/Offline Signature Schemes,” Proc. CRYPTO, pp. 355-367, 2001.