Egyptian Informatics Journal 22 (2021) 317–328

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Efficient privacy-preservation scheme for securing urban P2P VANET networks

Bechir Alaya *

Department of Management Information Systems and Production Management, College of Business and Economics, Qassim University, 6633, Buraidah 51452, Saudi Arabia
IResCoMath Laboratory, University of Gabes, Tunisia

ARTICLE INFO

Article history:
Received 26 August 2020
Revised 19 October 2020
Accepted 4 December 2020
Available online 26 December 2020

Keywords:
UP2PVANET
Security
Homomorphic encryption
Privacy-preserving
Black hole attacks

ABSTRACT

To meet the performance and security challenges for users who have the same interests in the urban Peer-to-Peer VANET environment (UP2PVANET), the confidentiality & security scheme applied to the urban P2P VANET network (CSP2P) is introduced which helps maintain an effective certification framework. An intelligent cooperative detection system is also proposed, that uses homomorphic encryption to detect routing attacks. To validate the effectiveness of proposition CSP2P, it is integrated into the implementation of the AODV routing protocol. Simulations results showed the efficiency of the CSP2P scheme in terms of black hole detection, in terms of transmission delay, thanks to the in-depth performance evaluation in the UP2PVANET environment. The obtained results prove that the proposed scheme will allow an increase in system performance of nearly 10% under all load conditions.

1. Introduction

Over the past decade, vehicular ad hoc networks (VANETs) have become one of the most suitable dynamic wireless topologies for the enterprise world [1]. Urban VANETs are highly mobile ad hoc wireless networks that have been implemented to provide passenger safety, driver assistance, and emergency alert services. VANET is designed to guarantee self-organized vehicle training, i.e. decentralized vehicle-to-vehicle communication (V2V) and the infrastructure-based vehicle network, i.e. vehicle centralized to infrastructure (V2I) at a time [23].

The urban VANET network contributes to a large quantity of network traffic, due to many vehicle users (VU) share or uses data massively. A large number of applications from VANET networks are currently used such as real-time streaming services and video on demand (VoD) [4]. Several techniques for sensor networks [5], eHealth systems [6 7], vehicle communications [8], and intelligent network communications [9] have been proposed. However, these proposed schemes do not take into account the confidentiality of users of VANET networks and no longer take into account dynamic topology, limited bandwidth, limited physical security, and energy use. Therefore, it is essential but difficult to design an effective system preserving the security and confidentiality of VANET networks.

Due to the mobility of the vehicle user, users can often communicate with others on a VANET network or with the Peer-to-Peer (P2P) network exchange node [10]. It will be possible for several VUs to share their resources which are easily accessible via P2P or VANET or among themselves, provided that these VUs also share the same interests (such as multimedia data, e-books, etc.). The last communication type is called Urban P2P VANET networks (UP2PVANET).

Let U which represents all users, for each user$VU_i \in UP2PVANET$, let$Sim(VU_i)$ the similar interests of VU_i, and $Soc(VU_i)$ represents the sociality of VU_i, and defined as follows:

$$Sim(VU_i) = \begin{cases} 1 \text{ if } VU_i \text{ is sociable;} \\ 0 \quad \text{otherwise.} \end{cases} \quad (1)$$

When two users $VU_i, VU_j \in U$ contact each other, the conditions necessary for establishing a social relationship based on the same similar interests are as follows:

$$\begin{cases} Soc(VU_i) = Soc(VU_j) = 1, VU_i, VU_j \text{ are sociables;} \\ Sim(VU_i) = Sim(VU_j) \quad \text{have the same similar interests.} \end{cases} \quad (2)$$

* Address at: MIS Department, College of Business and Economics, Qassim University, Al-Mulida Road, North Prince Nayef Airport, Qassim, KSA, Saudi Arabia.
E-mail address: b.alaya@qu.edu.sa

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

https://doi.org/10.1016/j.eij.2020.12.002
1110-8665/

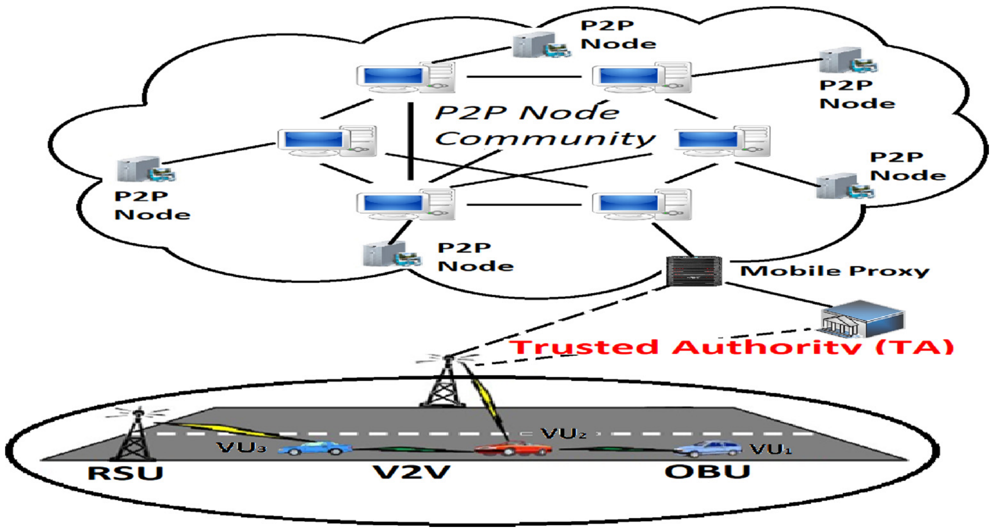

Fig. 1. The UP2PVANET system model.

In this work, the UP2PVANET network is considered, composed of a single TA (trusted authority), a large number of vehicle users $VU = \{VU, VU_2, \cdots, VU_n\}$ in an urban VANET network, and a P2P node group, as shown in Fig. 1. In the UP2PVANET network, the routing of data packets can lead to problems such as the misuse of network bandwidth, network overload resulting from loss and delay of data, loss of vision, etc.

This is why an effective certification scheme is proposed. Such that, the mobile proxy (MP) send to VU_i node the certificate and private key. Based on the proxy re-signature cryptography technology [1112], the node VU_i can re-sign the certificate and can also verify the certificate.

To face security and performance problems, a secure and intelligent detection scheme is also introduced with a strong preservation of confidentiality, which permits a UP2PVANET user to receive and share data packets securely.

Obviously, in a UP2PVANET environment, the speed and dynamicity of the vehicles are arbitrary, which makes the traffic necessarily dynamic and arbitrary. Vehicles have been made "intelligent" by adding new functions to understand their environment through sensors, to communicate with other vehicles using wireless or 5G radio interfaces, to process this information, and make decisions about vehicle behavior using an on-board computer. Finally, to validate the security of our CSP2P scheme, the security properties of the proposed scheme are analyzing and simulate it in two different scenarios. In the first scenario, the simulation results demonstrate that with a configuration of our proposed diagram where the attack is launched on a certain number of jumps, besides, more detections of black hole attack are presented. To achieve the practicality of our scheme, the performance of MP is also thoroughly assessed.

The rest of the article is organized as follows: Section 2 highlights the existing that applies video streaming over Peer to Peer Network and VANET network, and privacy-preservation and security schemes to the VANET network in the literature. Section 3 describes the application of our CSP2P scheme video data replication model and presents our replication algorithm. Section 4, presents a security analysis of the proposed CSP2P scheme. Section 5 evaluates the solution based on simulation results analysis. Finally, Section 6 concludes the paper and recommends many guidelines for future analysis.

2. Review of related work

This section reviews the main existing work found in the scientific literature that applies video streaming over Peer to Peer Network and VANET.

2.1. Video streaming over Peer to Peer

P2P (Peer-to-Peer) network contributes to a large exchange of data of different types [5] between the P2P users. Due to user mobility, users can often communicate with others over ad hoc networks such as VANET or with P2P network exchange node.

In [13], focusing on real-time streaming and video-on-demand in wireless networks, the authors examined a generic P2P video streaming system. Another similar study was proposed in [14] by considering the core layer and cross-layer techniques in wireless networks and based on resilient techniques for P2P video streaming.

In [15] the authors suggested a P2P video streaming service based on multiple hosting (M−HH−P2P) to obtain an optimal QoE. Based on the grouping which distributes the video segments evenly, they also suggested a new storage strategy. Using speculation, a prefetching mechanism has been proposed to obtain a smooth reading, its mathematical model is as follows:

$$P_{rr'} = \{k_r | k_{r'}\} = \frac{g_{rr'} + FIA_{rr'}}{\sum k_r + FIA_{rr'}} \tag{3}$$

Such as $P_{rr'}$,represents the association probability between the node $r and r'$, $g_{rr'}$ is the association between segment k_r and segment $k_{r'}$, and $FIA_{rr'}$ is the frequency increment from the association of segment k_r to any other segment $k_{r'}$.

Evenly, a routing scheme for P2P live broadcast networks has been proposed in [16]. To increase the visualization quality of video and network throughput, the proposed scheme uses a video data integration mechanism with random network coding. It is a push–pull mesh that gives higher priority to the basic video layers for P2P transmission. However, video data may be lost during communication due to the missed deadline or noise, and many others.

2.2. Video streaming over VANET

VANET networks can treat vehicles as mobile detectors of the road situation in real-time [1718]. In [19], the authors deal with live multimedia streaming in dynamic and loss VANETs using network coding at the symbol level. Streaming data is disseminated from sources considered to the vehicles concerned via a transfer approach. This approach is based on the management of selected distributive relays. The authors use packet-level network coding (PLNC) instead of symbol level network coding (SLNC). The authors of [11] focus on multimedia streaming using a dynamic overlay approach in urban VANETs. They claim that an overlay multicast is more robust than the others. The approach is called Overlay Multicast in VANETs (OMV) and improves the stability of the overlay. The improvements are obtained by using two strategies, which are the QoS satisfied dynamic overlay and the mesh structure overlay. Thanks to the results of the evaluation in VANET networks, the OMV considerably reduces packet loss. This approach also decreases the end-to-end delay. QoS for VoD in urban VANET based on a hierarchical multi-hosted P2P architecture is discussed in [20]. Indeed, the authors propose an effective user-centered mobile VoD solution called "QUVoD" in a VANET. This solution offers a high level of QoS to passengers. Also, the authors introduce four new mechanisms. It is a distributed schema for storing video segments, a schema for finding video segments, delivering data using multipath, and a strategy based on speculation prefect. In [21], the authors propose an adaptive multimedia streaming system for vehicle networks. The proposed scheme takes into account the problems of frequent vehicle mobility, the volatility of the network environment, and the uneven distribution of roadside BS.

The nodes' density, the nodes' speed, and the pause times were also analyzed in [22], during the application of (AODV) and (DYMO) in different scenarios of VANET network traffic. In VANET, route failures are frequent because of the nodes which join and leave the network randomly. A comparative analysis has shown better results with AODV in terms of conversation time, medium opinion score (MOS), and jitter. To see the advantages of one over the other, VOIP applications can be implemented with other routing protocols such as DSR (Dynamic Source Routing), and LAR (Location Aided Routing).

In [23] the authors used QoS performance models to assess the quality of video transmission over VANET. This is an analysis of the probability of connectivity, of the PSNR, and frame loss rate, with the application of certain routing protocols such as AODV, GPSR, and DSDV.

In [24], they proposed a method for selecting a group of Rebroadcasted (ReViV) strategic selective broadcast nodes for video streaming in VANETs. They introduced a new metric called diffusion capacity (DC) to classify vehicle nodes. In an environment of fully and intermittently connected networks [2526], ReViV was compared to other video streaming mechanisms and provided a lower end-to-end transmission delay, a lower frame loss rate, and a higher video transmission rate.

2.3. Privacy-preservation and security schemes to the VANET network

Many researchers aim to reduce the costs of attacks and security breaches in VANETs [272829]. The use of homomorphic encryption is quite low in VANETs [30]. A diagram relating to HE in VANET has been proposed in [31]. They used an algorithm adopted on an algebraic circuit with a low multiplicative degree of probabilistic decryption. The complexity was a bit ready$\widetilde{O}(\lambda^{3.5})$ knowing that λ represents a security parameter. In [31], another scheme was proposed to avoid the estimation based on the distance of the vehicle in the VANET, the authors proposed a multi-party security system with FHE.

The authors of [32] reduced the size of the public key to $\widetilde{O}(\lambda^7)$ based on FHE with integers, and later in other works they reduced the size of the public key to $\widetilde{O}(\lambda^5)$, as in the case of [33]. And to reduce the asymptotic complexity from $\widetilde{O}(n^{2.5})$ to $\widetilde{O}(n^{1.5})$, the authors of [34] introduced a fully homomorphic scheme with priming functionality. In [35] they deciphered the messages and they reduced the overload by using FHE with a p006Flylog of size $\widetilde{O}(\lambda)$ and depth (λ).

In [36], the authors used the public key homomorphism property. On the other hand, in [37], They proposed a scheme with a computational complexity of $k\hat{A} \cdot \mathrm{polylog}(k) + \log|DB|$pieces, based on short vector problems.

Other FHE techniques have been proposed such as FHE secured with two multi-key identities FHE [38], threshold FHEs with the monotonic Boolean formula [39], diagram, algebraic FFEs with multivariate polynomials [40], and FHEs with sorting on encrypted data without decryption [4142]. Wang et al. have used FHE in [43] with reduced time for encryption, decryption, and re-encryption with Fast Fourier Transform. In [44], challenges on integers have been implemented with a simple FHE to optimize complexity. Fan et al. have proposed an algorithm [45] which takes into account the FHE which uses the errors (LWE) for the practical adjustment with automatic learning. Operators of classical integer manipulation like bit shift, arithmetic, comparison, logic, etc. have been used on BGV-style cryptosystems in [4647].

2.4. Comparison study

However, the proposed schemes must be more attractive to be deployed in vehicular networks, in particular with its tendency to establish almost latency-free communication, no more concerns about bandwidth capacity, very high speed, etc. Also, with the majority of the approaches proposed, the case of dense vehicles remains a critical concern and one which requires the efficient use of existing systems and more efficient safety schemes. This can cause message delay/loss, additional communication costs, and heavy load overload on high mobility roads or dense roads when vehicles need to change frequently. Several proposals should also detect, prevent, and inform elementary and compound attacks to ensure sustainable communication between its neighbors and improve the availability of content and minimize the loss rate of video segments. Therefore, it is necessary to propose a new scheme to address the problems of the unpredictable arrival of vehicle nodes and security and confidentiality requirements. Besides, the proposed system always remains tough in the face of the high mobility of vehicle nodes and their frequent changes.

3. CSP2P scheme to UP2PVANET network

In this section, the confidentiality & security scheme is applied to the urban P2P VANET network (CSP2P). However, everything concerns the state of the various components of the UP2PVANET network, especially the vehicle nodes. The application of our scheme varies according to attack types, authentication of vehicle nodes, and the integrity and confidentiality of the video data.

The CSP2P scheme is based on six phases: 1) Initialization phase; 2) Key and certificate sent by TA; 3) The certificate update in the CSCNET scheme; 4) verification and signature; 5) the requested response; and 6) Response to the attack detection demand.

Table 1
The cost of necessary operations in the CSP2P scheme.

Curve	**CP-80** [63]		**MNT-80** [65]		**BN-128**[66]	
$\mathbb{G}_2$	$\mathbb{F}_\varepsilon$		$\mathbb{F}_{\varepsilon^3}$		$\mathbb{F}_\varepsilon$	
k	2		6		12	
Modulus (bits)	512		160		256	
Paring curve type	Tate [62]		Ate [64]		Tate [62]	
With/Without precomp.	with	without	with	without	with	without
MesDem Authentication	0.185 ms	1.254 ms	0.565 ms	2.611 ms	0.954	1.024
Encrypt	0.215 ms	1.372 ms	0.156 ms	0.941 ms	0.398	1.254
Decrypt (2 parings)	1.059 ms	2.720 ms	1.162 ms	2.773 ms	3.265	3.874
Decrypt (multi-pairing)	0.611 ms	2.328 ms	0.827 ms	3.587 ms	2.117	3.028

3.1. Homomorphic encryption and identity-based signature

3.1.1. Homomorphic encryption

Formally, a homomorphic encryption scheme is the data of four probabilistic algorithms $(KeyGen, Enc, Dec, Eval)$ which run in polynomial time and function as follows:

A *KeyGen* key generation algorithm takes as input a security parameter 1^λ and returns public parameters K, a secret key ky, and a public key Pky.

An *Enc* encryption algorithm which takes as input the public parameters K, a clear message r, the public key Pky, and returns an encrypted$E = Enc(K, Pky, m)$.

A decryption algorithm *Dec* which takes as input the public parameters K, an encrypted E, the secret key ky, and returns a message $m' = Dec(K, ky, E)$.

An evaluation algorithm $Eval$ which takes as input the public parameters K, the public key Pky, a circuit C defined on n, encrypted $(E_1, E_2, \cdots, E_n)$ relating to the messages $(m_1, m_2, \cdots, m_n)$ respectively. It returns an encrypted $E = Enc(K, Pky, C(m_1, m_2, \cdots, m_n))$.

The public parameters K often include the re-linearization key which is used by the $Eval$ algorithm to control the encryption expansion. In the case of a completely homomorphic scheme, K also contains encryption of the secret key which is used. Note also that, a bilinear coupling is an application $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_Z$ having three properties, i.e., computable, bilinear, and nondegenerate as detailed in [48].

In our work, the public key in HE is (M, f), and the corresponding private key is (α, β). Let $E(\cdot)$ that represents the encryption function, a message m, and a random number x. The cryptogram will then be as follows:

$$C = E(m) = f^m \cdot x^M modM^2 \tag{4}$$

When the function $(y) = (y - 1)/M$, the homomorphic property additive is defined as follows:

$$E(m_1) \cdot E(m_2) = \left(f^{m_1} \cdot {x_1}^M\right)\left(f^{m_2} \cdot {x_2}^M\right) modM^2$$

$$= f^{m_1+m_2} \cdot (x_1x_2)^M modM^2 \tag{5}$$

$$= E(m_1 + m_2)$$

Also, hash chains [4950] are used that are one-way functions.

3.1.2. Signature-based on identity

The signature-based on identity is defined by the bellow algorithms:

Config: The private key generator (G_{pk}) first chose two groups $\mathbb{G}_1 and \mathbb{G}_2$ of the first-order $k > 2^\lambda$ with λ is the security parameter. Then G_{pk} chooses the generator T of $\mathbb{G}_1$ and the random master key $mk \in \mathbb{Z}_k^*$ and calculates the associated public key $pk = mk \cdot T$. It also takes on the cryptographic hash functions $CH_1, CH_2 : \{0,1\}^* \rightarrow \mathbb{G}_1{}^*$. The public system parameters are $(k, \mathbb{G}_1, \mathbb{G}_2, e, CH_1, CH_2)$.

Key generation: either Ui is the user identity, the G_{pk} calculates $\varrho_{Ui} = CH_1(Ui) \in \mathbb{G}_1$ and the associated private key $A_{pk} = mk \cdot \varrho_{Ui} \in \mathbb{G}_1$ that is transmitted to the user.

Signature: to sign a message, the user chooses a random number $r \in \mathbb{Z}_k^*$, and calculates $X = r \cdot T, Y = A_{pk} + r \cdot CH_2(Ui, M, X)$. The signature on M will be the couple $\mu =< X, Y >$.

Verification: To verify the signature $\mu =< X, Y >$on a message M for the user identity Ui, the verifier accepts the signature if $e(T, Y) = e(pk, CH_1(Ui))e(X, CH_2(Ui, M, X))$.

3.2. Initialization phase

To initialize the entire system, it is assumed that there is a Trusted Authority (TA). For the routing protocol, AODV is adopted, which represents one of the best-known protocols in the family of reactive routes [51]. Two control messages are initialized by each node $\mathrm{VU} = \{\mathrm{VU}, \mathrm{VU}_2, \cdots\}$ of UP2PVANET, such as *{MesDem, MesRes}*. These messages have the format of the "RREQ route request" message [52]. Such that each message consists of three parts, the general communication costs, the verification costs, and the signature costs (see Table 1). Either the bilinear parameters $(k, T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_Z, e)$. Then, the system will be initialized by the TA by performing the following steps.

1) TA chooses a secret key and a secure symmetric encryption algorithm $Enc_{sy}(.)$, and three secure hash functions $CH_1, CH_2, andCH_3$, where $CH_1 : \{0,1\}^* \rightarrow \mathbb{G}_1, CH_2 : \{0,1\}^* \rightarrow \mathbb{G}_2, CH_3 : \mathbb{G}_Z \rightarrow \mathbb{Z}_k^*$. Also, the TA chooses a random number x in $\mathbb{Z}_k^*$, and calculates $\mathscr{T} = x \cdot Tand\mathscr{C}_{TA} = x \cdot CH_1(Ui_{TA})$, Such as Ui_{TA} represents the identity chain of the TA.
2) According to the confidentiality requirements of most nodes, the TA chooses $\Delta\varepsilon$ and defines the certificate validity period of $\Delta\varepsilon$. Then, and according to the density of the MP: in each domain, the TA decides the certificates that must update from an MP.
3) TA calculates the corresponding private key (α, β), and the public key of the Homomorphic encryption (M, f).
4) TA keeps the master key $(\alpha, \beta, mk, \mathscr{C}_{TA}, x)$ as secret, and shares the system parameters in UP2PVANET:
5) $P_{pub} = \{k, T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_Z, e, \mathscr{T}, CH_1, CH_2, CH_3, M, f, Enc_{sy}(.), \Delta\varepsilon\}$
6) When $MP_i(i = 1, \cdots, n)$ registers in the system, TA calculates the private key based on identity $SK_{MP_i} = xCH_1(ID_{TA} \| ID_{MP_i})$, where $ID_{TA}$is the identity chain of TA, $ID_{MP_i}$is the identity chain of MP_i, and SK represents the session key which is semantically secure [53], and which serves as a necessary condition for the confidentiality of the receiver session. Then, the TA sends SK_{MP_i} to MP_i via a secure channel.

3.3. Key and certificate sent by MP

When a new vehicle node VU_i wishes to communicate with other vehicle nodes in the domain Cl_j, the MP_i delivers the private

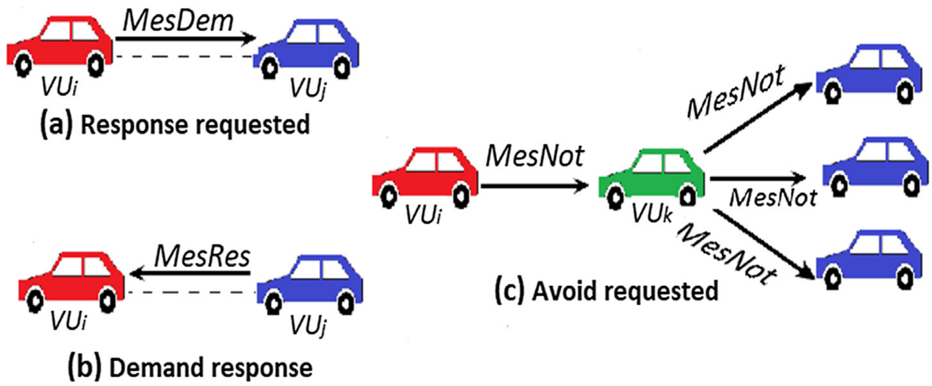

Fig. 2. Detection scheme based on neighbor × neighbor cooperation.

key SK_{VU_i} and the certificate $Cert_{MP_i,VU_i}$ as shown in the following list :

1) The MP_i chooses a random number x_{MP_i} in $\mathbb{Z}_k^*$ as the master key, and calculates the pseudo-identity $PI_{VU_i} = Enc_{x_{MP_i}}(ID_{VU_i})$, the private key $SK_{VU_i} = x_{MP_i}CH_1(ID_{MP_i}\|PI_{VU_i})$, and the public key $pk_{VU_i} = x_{MP_i}T$, where ID_{VU_i} is the identity chain of VU_i and ID_{MP_i} is the identity chain of MP_i. Then the MP_i calculates his private point $\mathcal{T}_{MP_i} = x_{MP_i}T$ and $T_{MP_i} = xCH_1(ID_{MP_i})$.
2) MP_i generates the certificate $Cert_{MP_i,VU_i} < pk_{VU_i}, R >$, with $R = PI_{VU_i} + x_{MP_i}CH_2(ID_{MP_i}, SK_{VU_i}, PI_{VU_i})$.
3) MP_i sent $SK_{VU_i}$and $Cert_{MP_i,VU_i}$ to VU_i via a secure channel.

3.4. Attack detection

Our CSP2P scheme uses the neighbor × neighbor cooperation mechanism (CNN) based on {*the response to the request and the response requested*} to detect attacks (see Fig. 2).

3.4.1. The requested response

Adversary node can send false messages by creating private communication tunnels., i.e., black hole attack. However, each node $VU_i \in UP2PVANET$ runs Algorithm. 1 to initiates a response request for nodes VU_i, and to execute the notification phase it waits for the response to its request. This phase is summarized by the following steps:

1) The node VU_i signs the message *MesDem*with the public key $pk_{VU_j} < f_{VU_j}, VU_{VU_j} >$ of the receiving node VU_j and the random number x_{VU_j} in $\mathbb{Z}_k^*$. (See Algorithm.1)
2) VU_j waits for short inter message time to run out, to avoid collisions. Then, based on its routing table, it selects all 1-hop nodes to send him messages.
3) After having received a message from VU_j node, VU_i extracts the response message MesResencrypted from *Cl*. Then the node VU_i extracts $Cert_{MP_i,VU_j}$ from MesRes and checks the validity of the certificate with MP_i (See Algorithm 2).
4) According to the certificate $Cert_{MP_i,VU_j}$ it decides that the link with node VU_j is proven if $Cert_{MP_i,VU_j}$ is valid. Else, it decides that the link with node VU_j is not proven.

Algorithm. 1: The requested response algorithm

Input: *Current timestamp &MesDem*
1) *Select a random number* x_{VU_i} in $\mathbb{Z}_k^*$
2) *Calculates: Cp that represents ciphertext of MesDem -* $Cp = E(MesDem) = f_{VU_i}^{MesDem} \cdot x_{VU_i}^{VU_{VU_j}} modVU_{VU_j}^2$ *Such as* $pk_{VU_j} < f_{VU_j}, VU_{VU_j} >$
3) ***for*** *each* $VU_j \in 1 - hopofVU_i$***do***
4) *Select the shortest time between two messages* (τ)
5) *Send_Request* (Cp, VU_j)
6) ***EndOutput***: *The ciphertextCp*

Algorithm. 2: The demand verification algorithm

Input: *The ciphertext C*
1) *When the node* VU_i *receive the ciphertext C*
2) *Recover MesRes from the ciphertext C*
3) $MesRes = L\left(C^{\alpha modVU_{VU_j}^2}\right) \cdot \beta modVU_{VU_i}$
4) *Where* $SK_{VU_i} < \alpha, \beta >$ *from MesRes*
5) *Recover* $Cert_{MP_i,VU_j}$ *from MesRes*
6) *Checks the certificate* $Cert_{MP_i,VU_j}$ *with* MP_i
7) ***If*** $Cert_{MP_i,VU_j}$ *is not valid* ***then***
8) *return not proved*
9) ***else***
10) *return proved*

Output: *proven or not proven link*

3.4.1.1. Response to the request. As the requested attack detection response, VU_j decides to execute the Algorithm. 3 when it receives the detection request. This phase of response to the request is represented as follows:

1) VU_j node recovers $Cert_{MP_i,VU_i}$ from *MesDem* and validates the certificate with MP_i (See Algorithm. 3).

2) CSP2P scheme executes the Algorithm. 1. in the case of the certificate $Cert_{MP_i,VU_j}$is not valid. In the other case, VU_j signs the message *MesRes* with $pk_{VU_i} < f_{VU_i}, VU_{VU_i} >$of the transmitter node VU_i and the random number x_{VU_i} in $\mathbb{Z}_k^*$.
3) The node VU_j waits for the time of requested attack detection response to run out and sends the encrypted text D. (See Algorithm 3, lines 12 to 13)

Algorithm. 3: The Request-Response algorithm

Input: *The control message MesRes, the ciphertext C, and* VU_i
1) *When the node* VU_i *receive the ciphertext C*
2) *Recover MesRes from the ciphertext C*
3) $MesRes = L\left(C^{\alpha mod VU_{VU_j}^2}\right) \cdot \beta mod VU_{VU_j}$
4) *Where* $SK_{VU_i} < \alpha, \beta >$
5) *Recover* $Cert_{MP_i,VU}$ *from MesDem*
6) *Checks the certificate* $Cert_{MP_i,VU_i}$ *with* MP_i
7) ***If*** $Cert_{MP_i,VU_i}$ *is not valid* ***then***
8) requested response (.)
9) ***else***
10) *Select a random number* x_{VU_j} in $\mathbb{Z}_k^*$
11) *Calculates: Cp that represents ciphertext of MesRes* - $Cp = E(MesRes) = f_{VU_i}^{MesRes} \cdot x_{VU_j}^{VU_{VU_i}} mod VU_{VU_i}^2$ *Such as* $pk_{VU_i} < f_{VU_i}, VU_{VU_i} >$
12) *Select the shortest time between two messages* (τ')
13) *Send_Request* (Cp, VU_i)
14) ***End***

Output: *The ciphertextCp*

3.5. Evolution of the certificate

The identity chain ID to $ID\|t$ is only valid before the specified expiration date t for a VU_i node. After the expiration of t, if a new certificate is not generated by MP_i, the corresponding certificate $Cert_{MP_i,VU_i}\|t$ is revoked. For this, CSP2P uses proxy re-signature cryptography technology [54], to adopt an efficient recovery strategy.

- VU_i removes the adversary node VU_x in its 1-hop routing table, in the case where VU_idecides that the link with the $VU_x$is unproven. As shown in the Fig. 2 (c), VU_i sends complaints to all its neighbors. When the neighbor node receives the claim (notification request), then it removes $VU_x$from its routing table. Finally, as shown by the Algorithm. 4, the neighbor node sends a complaint to all nodes belonging to its routing table.

Algorithm. 4: The avoid_requested algorithm

Input: *MesNot, and* VU_i
1) ***If*** $(VU_i \in (1 - hopofVU_x))$ ***then***
2) *Remove* VU_i*from the routing table of* VU_x
3) *Select* $x_{VU_i}(thatrepresentsarandomnumber)$ in $\mathbb{Z}_k^*$
4) ***for*** *each* $VU_z \in 1 - hopofVU_x$ ***do***
5) *calculate E the ciphertext of MesNot*
6) $E = E(MesNot) = f_{VU_z}^{MesNot} \cdot x_{VU_x}^{VU_{VU_z}} mod VU_{VU_j}^2$
7) *Where* $pk_{VU_i} < f_{VU_z}, VU_{VU_z} >$
8) *Select the shortest time between two messages*
9) *Send_Request*(E, VU_z)

Output: *The ciphertextE*

- Once the CSP2P scheme is successful, VU_i and VU_j nodes can give mutual support to other neighbors, and also can share experiences and information safely, using the evolution of the certificate. Thanks to these promising features, UP2PVANET can be widely used by multiple vehicle users. Besides, as shown in the Algorithm. 5, because the Access Point (AP) is not always available to a vehicle user in an urban VANET environment, active vehicle users, based on similar relationship interests can also help their friends of vehicle nodes to relay their data (multimedia data, textual data, etc.).

Algorithm. 5: Collaborative Information algorithm

Input: *status of AP*
1) *Vehicle user* VU_i*periodically collect information* Inf_i
2) ***If*** *an AP is nearby available,* ***then***
3) VU_i *immediately select Inf to P2P Node group*
4) ***else if*** *a Vehicle User* VU_i *is nearby then*
5) ***if*** $(soc(VU_i) = soc(VU_j) \&\& sim(VU_i) = sim(VU_j))$ ***then***
6) VU_i*and*VU_j*exchange their data*
7) *Before* Inf_i*'s expiration:* VU_i *helps* Inf_i *when it encounters available access points; else, deleting*Inf_i
8) ***End if***
9) ***End if***

Output: *Information* Inf_i

---

4. Safety and resistance of CSP2P scheme

To ensure that the imitator resistance and detector resistance requirements are respected, it is necessary to must first focus on the safety analysis of our CSP2P scheme. Next, it will be necessary to focus on the evolution of UP2PVANET user certificates and also

Table 2
Format of the signed message "MesDem", "MesRes".

0										1										2							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
Type								J	R	G	D	U	Reserved											Hop Count			
MesDem ID																											
Destination IP Address																											
Destination Segment Number																											
IP Address of Source																											
Source Segment Number																											
Soc														Sim													
Certificate														Signature													

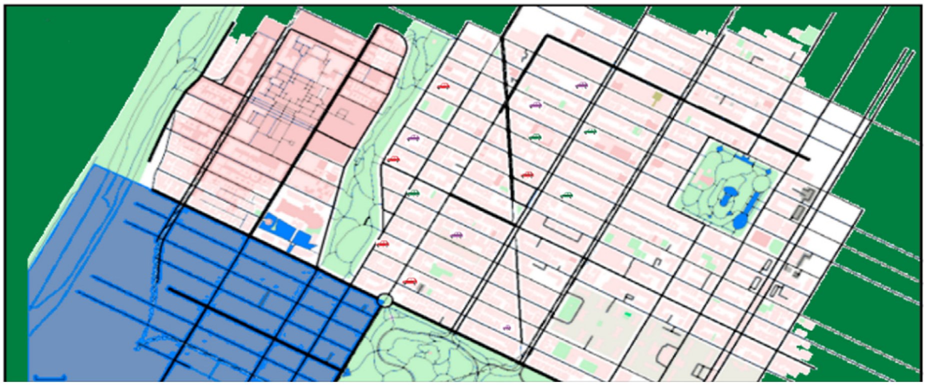

Fig. 3. Topology Urban VANET network from SUMO.

on how the CSP2P scheme will follow to ensure message confidentiality Table 2.

4.1. Semantic security of CSP2P scheme

Let a polynomial opponent $\mathscr{P}$ that try to take advantage of knowledge from the challenger $\mathscr{CH}$. According to the CSP2P scheme, $\mathscr{P}$ could follow the following rules: *1)* $\mathrm{R.Not}(\mathrm{Sk}_{pub}, \varepsilon)$ which permit $\mathscr{P}$ to get a public key of the signatory k_{pub}, a signature according to his choice on the message S, and a random value ε selected by $\mathscr{P}$; *2)* $\mathrm{R.Mod}(S, \mathrm{q}, \mathscr{L})$which is used by $\mathscr{P}$ to change the *message-signature (S, q)* with the $\mathscr{L}$ changes he wishes. The rule resend a valid and modified signature if the modifications are admissible on the error; *3)* $\mathrm{R.Prove}(S, \mathrm{q}, \mathscr{W})$permit $\mathscr{P}$ to obtain a justification of the origin *message-signature (S, q)* depending to $\mathscr{W}\{(\mathrm{m}_x, \mathrm{q}_x)\}_{x\in[1.k]}$ (database). *4)* $\mathrm{R.Not/Mod}_a(\mathrm{S}, \varepsilon, \mathrm{M})$ permit $\mathscr{P}$ to assume as input S, ε, and M. If $a = 1$, it modifies the original signature of the message S by M. Otherwise if $a = 0$, it resends S'as a message which corresponds to the message modified by M.

4.2. Confidentiality preservation

In CSP2P, it is a control messages based on homomorphic encryption [55], such as *{MesDem, MesRes}*. Even if $\mathscr{P}$ spies on the encrypted text, he can never sign the corresponding message. $\mathscr{P}$cannot get the message across, even if $\mathscr{P}$ compromises the MP_i database. Consequently, CSP2P guarantees confidentiality preservation.

4.3. Certificates evolution

In this phase, even if $\mathscr{P}$ is spying on the exchange between $MP_i andVU_i$, he cannot get the certificate information. Otherwise, even if $\mathscr{P}$ involves all certificates, it can never have an idea about the future and even current certificates. Notably, the evolution of the user security certificate is reached in CSP2P.

5. Experimental results and analysis

The simulation of the CSP2P scheme for the security and confidentiality of UP2PVANET is carried out via the NetSim version 10 simulator [56 57] and the MOEA framework [58] to optimize the parameters. The simulation experiments were carried out in two different scenarios, for different types of nodes to illustrate that the load between the nodes is balanced. All digital experiments are performed on the PC with Intel Core i7 and 8 GB of RAM. The MOEA framework is a java-based framework specialized in multi-objective evolutionary algorithms (MOEA) and the optimization phase of the approach has been carried out. However, the VANET simulation was performed in SUMO and NetSim. RSUs act as 802.11p wireless APs to communicate with vehicles in the coverage range and set the bandwidth to 1 Gbit/s. The performance measures are: *i)* The rate of Black Hole detection (Dr); *ii)* the mean *MesDem* reporting delay (MRD); and *iii)* the average transmission delay (t_{td}). Fig. 3 shows the transport map of a metropolitan region exported from OSM.

5.1. First scenario

In this first scenario. the aim is to assess the influence of CSCNET against the black hole attack on AODV reactive routing. It is random generated topologies of the urban VANET network with N nodes of mobile vehicles and 4 RSUs which are regularly deployed on a square field varying from $500 \times 500 m to 1500 \times 1500 m$ depending on the size of the UP2PVANET network, where N is between 30 and 80. The pair of adversary nodes is chosen randomly from among the nodes in the VANET network. In the case of 60 nodes, half ($30 nodes$) which have the same interests (SI_1) and the group of form $\mathscr{g}_1$, and the other half have the same interests (SI_2) and the group of form $\mathscr{g}_2$. Each node randomly selects a destination in the region using the shortest route and with speed δ. Moreover, let $\mathscr{R}^2$ the maximum transmission range. Let also, $\mathscr{P}_{\mathrm{n,Ne,Ad}}$ that indicates the probability that it exists at least n neighboring nodes in $\pi\mathscr{R}^2$ (the transmission range) of an adversary of surface Sr.

$$\begin{aligned}\mathscr{P}_{\mathrm{n,Ne,Ad}} &= \mathscr{P}\left(\mathrm{N} \geq \mathrm{n}|\pi\mathscr{R}^2\right)\\ &= 1 - \mathscr{P}\left(\mathrm{N} < \mathrm{n}|\pi\mathscr{R}^2\right)\\ &= 1 - \sum_{i=0}^{n-1}\mathscr{P}\left(\mathrm{N} = i|\pi\mathscr{R}^2\right)\\ &= 1 - \sum_{i=0}^{n-1}\binom{|\delta|}{i}\left(\frac{\pi\mathscr{R}^2}{Sr}\right)^i\cdot\left(1 - \frac{\pi\mathscr{R}^2}{Sr}\right)^{|\delta|-i}\end{aligned} \tag{6}$$

Let $\mathscr{D}_{bh}$ be the black-hole detection rate, which is expressed as follows:

$$\mathscr{D}_{bh} = \frac{1}{t_{\mathscr{D}}} \tag{7}$$

Such as $t_{\mathscr{D}}$ represents the time of the attack detection.

Let $\mathscr{s}_r$ be the social report of a group $\mathscr{g}$ with, $\mathscr{s}_r = \frac{ThenumberofsociableVU}{allVUin_{\mathscr{g}}}$ by supposing that the two $\mathrm{SI}_1 and \mathrm{SI}_2$ have the interest report$\mathscr{s}_r = [0.3, 0.4, 0.5, 0.6]$.

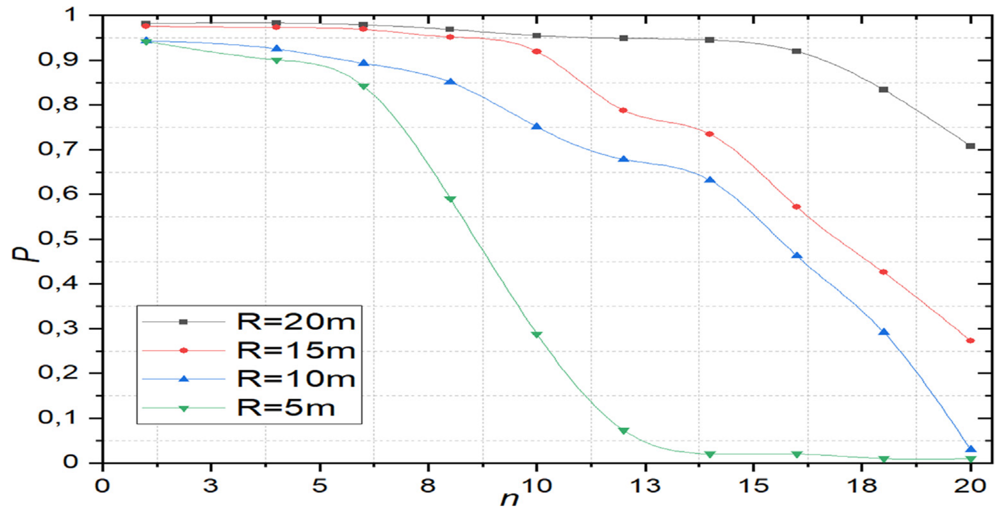

Fig. 4. The probability of n neighbors of an adversary $\mathscr{P}_{\mathrm{n,Ne,Ad}}$.

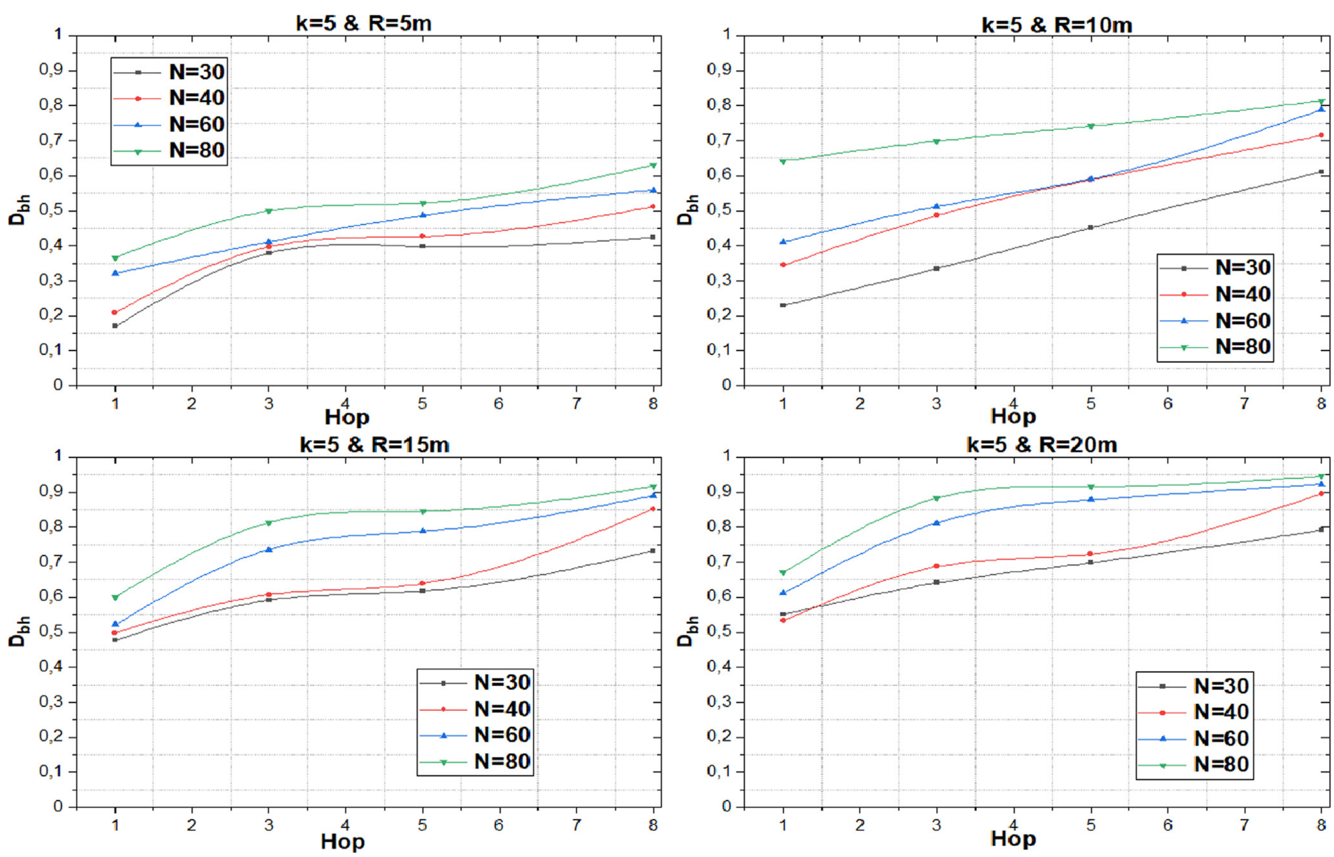

Fig. 5. Blackhole bond detection rate $\mathscr{D}_{bh}$ varying with the Hop (tunnel length).

Fig. 4 presents the probability of n neighbors of $\mathscr{P}_{\mathrm{n,Ne,Ad}}$ in a UP2PVANET network, with different values of n, $(1 \leq n \leq 20)$. With $n \leq 7$, it is clear that when n belongs to this interval, the predicted high probability of the black hole attack can be realized.

Fig. 5 illustrates the rate of detection of the black hole $\mathscr{D}_{bh}$ varying according to the length of the tunnel (Hop) which represents the interval of jumps between the adversaries, where: $\mathscr{R} \in [5, 10, 15, 20] and n = 5$. As shown in Fig. 5, $\mathscr{D}_{bh}$ increases with increasing $\mathscr{R}$ throughout the UP2PVANET network. When the attack is launched over several additional hops, note that $\mathscr{D}_{bh}$ is more detected. Also, from the same figure, note also that $\mathscr{D}_{bh}$will increase considerably with the increase of N.

Fig. 6 presents $\mathscr{D}_{bh}$ varying according to *Hello transmission protocol* [59] (H_{TP}) to discover the neighbors and check periodically the presence of neighbors, and the different durations of the black hole attack, such that $\mathscr{R} \in [5m, 10m, 15m, 20m] and n = 5$. Fig. 6 shows if the detection rate of the black hole is longer than its attack duration. Also, Fig. 6 show that the detection rate of $\mathscr{D}_{bh}$ increases in the whole UP2PVANET network, with an increase of $\mathscr{R}$. CSP2P takes longer to detect if the transmission interval $H_{TP}$is long

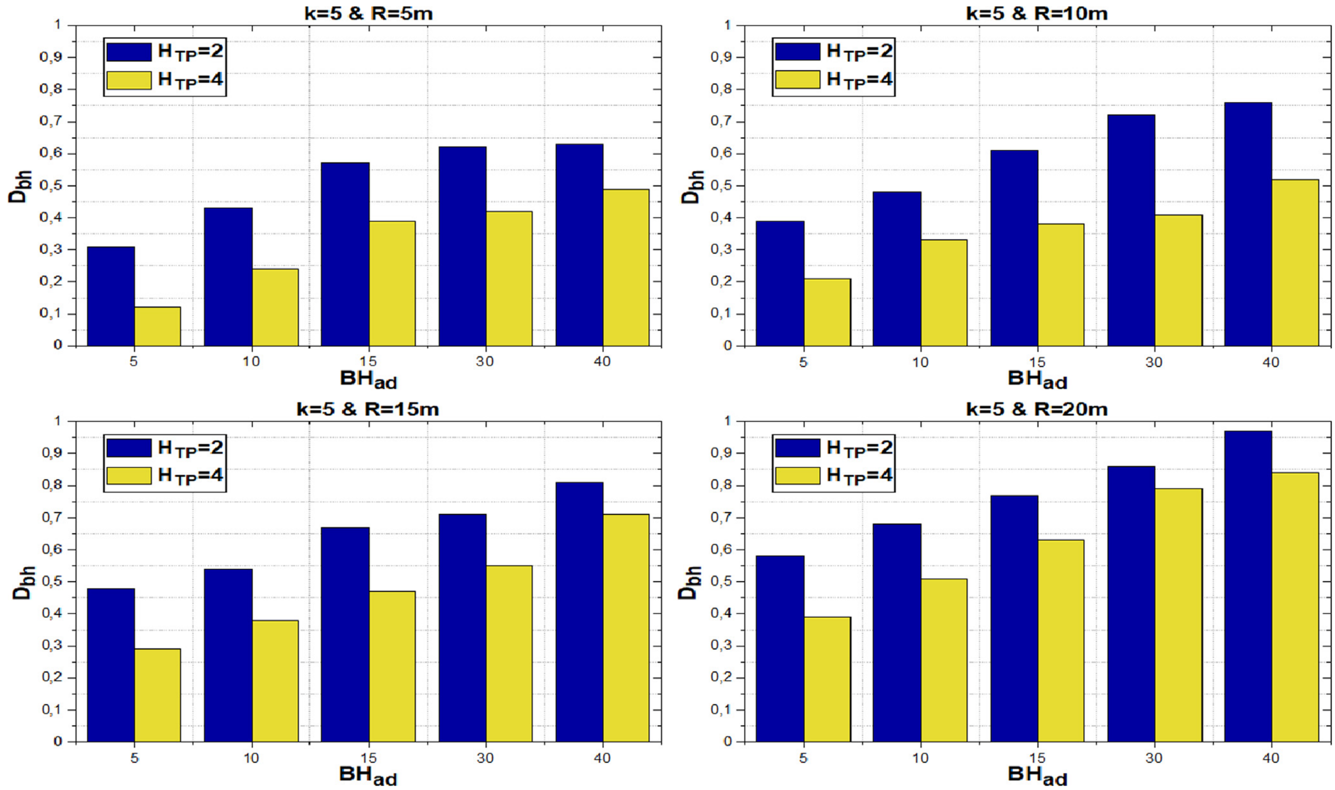

Fig. 6. Blackhole bond detection rate $\mathscr{D}_{bh}$ varying with the *Hello transmission* (H_{TP}) and black hole attack duration BH_{ad}.

enough. Therefore, the use of small message transmission intervals is more efficient for the CSP2P scheme.

5.2. Second scenario

In this scenario, the time required for a node to send messages (*MesDem* to reach its neighboring nodes via MP) is implemented, and which represents a very important performance measure in P2P systems and especially in UP2PVANET networks. Another metric that interests us in our CSP2P scheme is the transmission delay at the node level. The cost of calculating the CSP2P scheme mainly concerns these cryptographic methods: multiplication in $\mathbb{Z}^{*}_{t,}$encrypt, decrypt, hashing operations, and authentication. The results of the measurements are given in the Table 1. The homomorphic encryption of the predicates is adopted to internal products (IPE) [60], and the numbers obtained in the Table 1 [61], to estimate the cost calculation in CSP2P.

Tate pairing curve type [62] is used, with the integration degree $k=2$ Cocks-Pinch (CP-80) [63]. CP-80 is on $\mathbb{F}_{\varepsilon}$ with 512 bits of the first-order ε. Next, using the Ate paring curve type [64] with a degree of integration $k=6$Miyaji-Nakabayashi-Akano (MNT-80) [65]. MNT-80 is on $\mathbb{F}_{\varepsilon^3}$ with 160 bit of the first-order ε. Finally, using the Tate pairing curve type [62] with the integration degree $k=12$ Barreto-Naehrig (BN-128) [66]. BN-128 is on $\mathbb{F}_{\varepsilon}$ with 256 bits of the first-order ε.

The Poisson Input, Constant Service, Multiserver (M/D/1) [67] process are implemented to evaluate the transmission delay in our CSCNET scheme. Considering the starting rate μ, the average arrival *MesDem* at the node level follows a Poisson process with an arrival rate λ, and advancing the process from state$i$ to $i+1$. The time *MesDem* average delay before being put into the node buffer is t_v, which is as follows:

$$t_v=\frac{1}{\mu}\cdot\frac{2-\beta}{2-2\beta},\text{with}\beta=\frac{\lambda}{\mu} \tag{8}$$

The black hole attack results in a transmission delay. Also, the encryption and decryption operations cause the transmission delay, although they can be reduced by the broadcast of the message *MesDem*. Consider p the probability of an invalid message *MesDem* arriving at the node due to the black hole attack. Studying now the average waiting time in the node buffer.

Considering first the time it takes the i^{th}*MesDem* in the node to wait for the arrival of the next$(i+1)^{th}$*MesDem*. When a valid *MesDem* message is buffered at the node, then many *MesDem authentications* at the node level are presents, that represents a geometrically distributed random variable:

$$\mathrm{P}(k)=p^{k-1}(1-p) \tag{9}$$

Specifying t_w as the average waiting time, as follows:

$$t_w=\sum_{k=1}^{\infty}\frac{k}{\mu}\cdot p^{k-1}(1-p)=\frac{1}{\mu(1-p)} \tag{10}$$

With $w=1,2,\cdots,m-1$. In the case of $w=m\Rightarrow t_w=t_m=0$ Therefore, before sending the message *MesDem*, a waiting time of each *MesDem* in the node buffer is presents that will be:

$$T_j=\begin{cases}\frac{m-j}{\mu(1-p)},j=1.2,\cdots,m-1;\\ 0,j=m\end{cases} \tag{11}$$

The average waiting time is as flows:

$$T_j=\begin{cases}\frac{m-j}{\mu(1-p)},j=1.2,\cdots,m-1;\\ 0,j=m\end{cases} \tag{12}$$

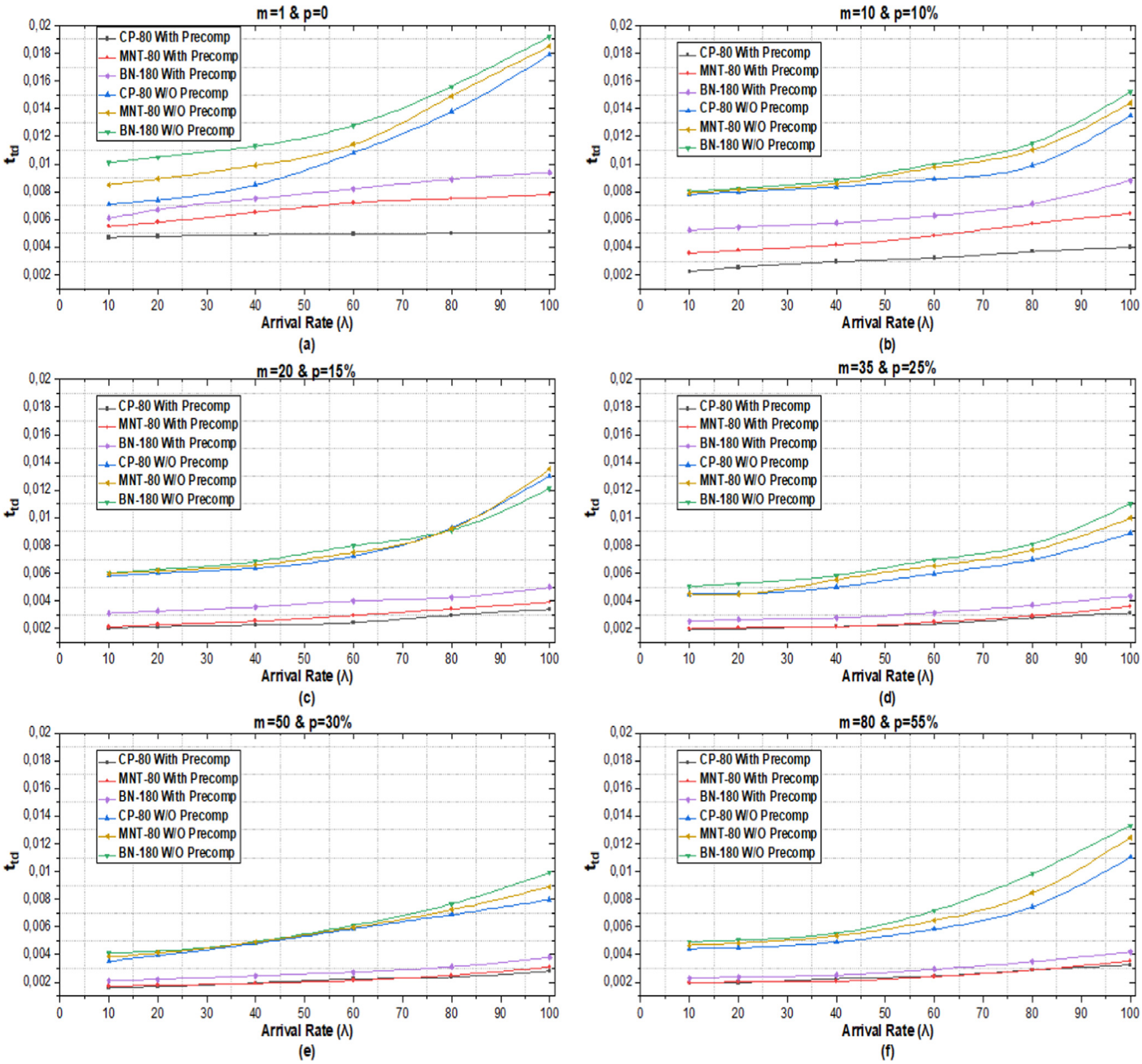

Fig. 7. Transmission delay t_{td} vs arrival rate λ.

The average waiting time is as flows:

$$t_w = \sum_{j=1}^{m} \frac{1}{m} \cdot T_j = \frac{1}{m} \cdot \frac{1}{\mu(1-p)} \cdot (1 + 2 + \cdots + (m-1))$$

$$= \frac{1}{m} \cdot \frac{1}{\mu(1-p)} \cdot \frac{m(m-1)}{2} \tag{13}$$

$$= \frac{1}{m} \cdot \frac{m(m-1)}{2\mu(1-p)} = \frac{m-1}{2\mu(1-p)}$$

Consequently, concluding that the transmission delay t_{td} from our CSCNET scheme to the node at the receiver is as follows:

$$t_{td} = t_v + t_w + t_d = \frac{2-\beta}{2\mu(1-\beta)} + \frac{m-1}{2\mu(1-p)} + t_d \tag{14}$$

Fig. 7. represent the average of the transmission delay t_{td} varying with λ of Poisson's process, where $1 \le \lambda \le 100$, and also fixing the parameters of m and from p. As shown in the Fig. 7 (a,b,c,d,e,f), overall t_{td} increases with the increase of λ. Also, the transmission delay t_{td} with the Miyaji-Nakabayashi-Takano curve (MNT-80) and the Barreto-Naehrig curve (BN-128) is greater than the Cocks-Pinch curve (CP-80). Furthermore, Fig. 7. roughly shows the relationship between t_{td} and p, m, such that the transmission delay t_{td} will also increase with the increase of *pandm*. Concluding also that with a more improved performance of a node, the transmission delay of *CP-80* can be considerably optimized.

6. Conclusion

In this paper, the scheme CSP2P is proposed as an intelligent scheme of detection of the black hole attack with the protection of video segments to secure the Urban Peer-to-Peer VANET network. CSP2P can not only meet the security and confidentiality requirements of the UP2PVANET network but can also detect, prevent, and inform elementary and compound attacks. The results of the theoretical and experimental analyses illustrate the effectiveness of our CSP2P scheme. This fact is confirmed by the reduction of delays for the VANET network and convergence towards a permanent regime and highly secure.

However, as one of our future works, for VANET networks, it will be useful to propose a new system preserving security and confidentiality using blacklists as follows:

- For each node in the VANET network, it maintains a blacklist that records all the identifiers of the nodes which they cannot successfully communicate in the previous period.
- For the system administrator, periodically, he will collect the blacklists of all the nodes. If the moments of appearance on the various blacklists exceed a predefined threshold, the system administrator revokes the legitimate authority.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Muhammad S, Jun L, Wensong W. Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. Wireless Communications and Mobile Computing 2020;31:1–25.
[2] W. Drira, K.h. Ahn, H. Rakha, F. Filali, ''Development and Testing of a 3G/LTE Adaptive Data Collection System in Vehicular Networks'', IEEE Transactions on Intelligent Transportation Systems, vol.17, 2016.
[3] Araniti G, Campolo C, Condoluci M, Molinaro A. LTE for vehicular networking: a survey. IEEE Commun Mag 2013;51(5):148–57.
[4] More S, Naik UL. ''Optimization driven Multipath Routing for the video transmission in the VANET,'' IEEE Global Conference on Wireless Computing and Networking (GCWCN). India: Lonavala; 2018. p. 6–10.
[5] Lu R, Lin X, Zhu H, Liang X, Shen X. BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Trans Parallel Distrib Syst 2012;23(1):32–43.
[6] C. Shekha, A. Khandakar, W. Hua, W. Frank, ''Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing''. IEEE Access. pp. 1-17, 2019.
[7] Janabi SA, Shourbaji IA, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal 2017;18(2):113–22.
[8] Liang X, Li X, Luan T, Lu R, Lin X, Shen X. Morality-driven data forwarding with privacy preservation in mobile social networks. IEEE Trans Veh Technol 2012;61(7):3209–21.
[9] Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy- preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst 2012;23(9):1621–31.
[10] Yang L, Li H. Vehicle-to-vehicle communication based on a peer-to-peer network with graph theory and consensus algorithm. IET Intel Transport Syst 2019;13(2):280–5.
[11] Ling HY, Wang K. Dynamic overlay multicast for live multimedia streaming in urban VANETs. Comput Netw 2012;56(16):3609–28.
[12] Xiaoliang W, Jianming J, Shujing Z, Liang B. A Fair Blind Signature Scheme to Revoke Malicious Vehicles in VANETs. Computers, Materials & Continua 2019;58(1):249–62.
[13] Masinde N, Graffi K. Peer-to-Peer-Based Social Networks: A Comprehensive Survey. SN Computer Science 2020;299:1–51.
[14] Abboud O, Pussep K, Kovacevic A, Mohr K, Kaune S, Steinmetz R. Enabling resilient P2P video streaming: survey and analysis. Multimedia Syst 2011;17:177–97.
[15] Xu C, Zhao F, Guan J, Zhang H, Muntean G-M. QoE-driven user-centric VoD services in urban multihomed P2P-based vehicular networks. IEEE Trans Veh Technol 2013;62:2273–89.
[16] Ayatollahi H, Khansari M, Rabiee H. A push-pull network coding protocol for live peer-to-peer streaming. Computer Network 2018;130:145–55.
[17] Hu M, Zhong Z, Ni M, Wang Z, Xie W, Qiao X. Integrity-oriented Content Offloading in Vehicular Sensor Network. IEEE Access 2017;5:4140–53.
[18] Zhangjie F, Lili X, Yuling L, Zuwei T. Privacy-Preserving Content-Aware Search Based on Two-Level Index. Computers, Materials & Continua 2019;59 (2):473–91.
[19] Zhenyu Y, Ming L, Lou W. CodePlay: Live Multimedia Streaming in VANETs Using Symbol-Level Network Coding. Wireless Communications, IEEE Transactions on August 2012;11(8):3006–13.
[20] Xu C, Zhao F, Guan J, Zhang H, Muntean GM. QoE-Driven User-Centric VoD Services in Urban Multihomed P2P-Based Vehicular Networks. Vehicular Technology, IEEE Transactions on Jun 2013;62(5):2273–89.
[21] Jung HC et al. ''An adaptive multimedia streaming dissemination system for vehicular networks. Applied Soft Computing'' 2013;13(12):4508–18.
[22] Yang X, Liu J, Zhao F. A vehicle-to-vehicle communication protocol for cooperative collision warning. Boston, MA, USA: IEEE Mobiquitous; 2004. p. 114–23.
[23] Xu S, Guo P, Xu B, Zhou H. QoS evaluation of VANET routing protocols. Journal of Networks 2013;8:132.
[24] A. Bradai and T. Ahmed, ''ReViV: Selective rebroadcast mechanism for video streaming over VANET,'' in Vehicular Technology Conference (VTC Spring), 79th IEEE, pp. 1-6, 2014.
[25] Yang J, Fei Z. Broadcasting with prediction and selective forwarding in vehicular networks. Int J Distrib Sens Netw 2013;9:309041.
[26] Cao D, Yuchen J, Jin W, Baofeng J, Osama A, Amr T, et al. ARNS: Adaptive Relay-Node Selection Method for Message Broadcasting in the Internet of Vehicles. Sensors 2020;20(5):1–18.
[27] Tyagi P, Dembla D. Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egyptian Informatics Journal 2017;18(2):133–9.
[28] Zhihua X, Lihua L, Tong Q, Jae SH, Xianyi C, Byeungwoo J. A Privacy-Preserving Image Retrieval Based on AC-Coefficients and Color Histograms in Cloud Environment. Computers, Materials & Continua 2019;58(1):27–43.
[29] Al Abdulkarim A, Al-Rodhaan M, Tian Y, Al-Dhelaan A. A Privacy-Preserving Algorithm for Clinical Decision-Support Systems Using Random Forest. Computers, Materials & Continua 2019;58(3):585–601.
[30] Wenbo S, Jiaqi W, Jinxiu Z, YuPeng W, Dongmin C. A Novel Privacy-Preserving Multi-Attribute Reverse Auction Scheme with Bidder Anonymity Using Multi-Server Homomorphic Computation. Intelligent Automation and Soft Computing 2019;25(1):171–81.
[31] D. Stehlé, R. Steinfeld, ''Faster fully homomorphic encryption''. Advances in Cryptology-ASIACRYPT, pp. 377–394, 2010.
[32] Song J, He C, Yang F, Zhang H. A privacy-preserving distance-based incentive scheme in opportunistic VANETs. Security and Communication Networks 2016;9(15):2789–801.
[33] Coron JS, Mandal A, Naccache D, Tibouchi M. Fully Homomorphic Encryption over the Integers with Shorter Public Keys. Crypto 2011;6841:487–504.
[34] JS. Coron, D. Naccache, M. Tibouchi, ''Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers''. In: Pointcheval D., Johansson T. (eds) Advances in Cryptology – EUROCRYPT 2012. Lecture Notes in Computer Science, Vol 7237. Springer, Berlin, Heidelberg, 2012.
[35] Gentry C, Halevi S. Implementing Gentry's Fully-Homomorphic Encryption Scheme. EUROCRYPT 2011;6632:129–48.
[36] C. Gentry, S. Halevi, NP. ''Smart, Fully homomorphic encryption with polylog overhead''. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 465–482. Springer, Berlin, Heidelberg, 2012.
[37] Boneh D, Gentry C, Gorbunov S, Halevi S, Nikolaenko V, Segev G, et al. In: Fully key homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. Berlin, Heidelberg: Springer; 2014. p. 533–56.
[38] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. SIAM J Comput 2014;43(2):831–71.
[39] Canetti R, Raghuraman S, Richelson S, Vaikuntanathan V. Chosen-Ciphertext Secure Fully Homomorphic Encryption. In: IACR International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer; 2017. p. 213–40.
[40] A. Jain, PM. Rasmussen, A. Sahai, ''Threshold Fully Homomorphic Encryption''. IACR Cryptology ePrint Archive, p.257, 2017.
[41] M. Tamayo-Rios, JC. Faugère, L. Perret, PH. Ho, R. Zhang, ''Fully Homomorphic Encryption Using Multivariate Polynomials'', IACR Eprint, 458, 2017.
[42] Lei X, Chungen X, Zhongyi L, Yunling W, Jianfeng W. Enabling Comparable Search Over Encrypted Data for IoT with Privacy-Preserving, Computers. Materials & Continua 2019;60(2):675–90.
[43] Kogos KG, Filippova KS, Epishkina AV. Fully homomorphic encryption schemes: The state of the art. In: In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian. p. 463–6.
[44] Wang W, Hu Y, Chen L, Huang X, Sunar B. Exploring the feasibility of fully homomorphic encryption. IEEE Trans Comput 2015;64(3):698–706.
[45] Chen Y, Nguyen PQ. Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers. EUROCRYPT 2012;7237:502–19.
[46] J. Fan, F. Vercauteren, ''Somewhat Practical Fully Homomorphic Encryption''. IACR Cryptology ePrint Archive, p.144, 2012.
[47] Jin W, Yangning T, Shiming H, Changqing Z, Pradip S, Osama A, et al. LogEvent2vec: LogEvent-to-Vector based Anomaly Detection for Large-Scale Logs in Internet of Things. Sensors 2020;20(9):2451.
[48] Fau S, Sirdey R, Fontaine C, Aguilar-Melchor C, Gogniat G. Towards practical program execution over fully homomorphic encryption schemes. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Eighth International Conference 2013:284–90.
[49] Yu Z, Yin L, Yifan W. Secure and Efficient Searchable Public Key Encryption for Resource Constrained Environment Based on Pairings under Prime Order Group. Security and Communication Networks. 2019;2019:1–14.
[50] Krawczyk H, Rabin T. Chameleon signatures. NDSS 2000. USA: California; 2000. http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/042.pdf.
[51] Agarwal P. Secure Node Communication With Cryptographic Algorithm in Vehicular Ad Hoc Networks. International Journal of Advanced Science and Technology 2017;109:1–12.

[52] Asit D, Martin K, Dinkar S. Dynamic Segment Replication Policy for Load-Balancing in Video-on-Demand Servers. IEEE Multimedia 1994;3(10):1–24.
[53] R. Lu, X. Lin, X. Liang, X. Shen, ''Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in vanet''. In GLOBE-COM, pp. 1-5, 2010.
[54] I. Toshiyuki, M. Nguyen, K. Tanaka, ''Proxy re-encryption in a stronger security model extended from CT-RSA2012''. Proceedings of The Cryptographers' Track at the RSA Conference, pp. 277-292, San Francisco, CA, USA: Springer Berlin Heidel- berg, 2013.
[55] B. Alaya, L. Laouamer, N. Msilini, ''Homomorphic encryption systems statement: Trends and challenges''. Computer Science Review. Vol. 36, May 2020.
[56] Garg A, Gupta M. ''Improving QoS by Enhancing Media Streaming Algorithm in Content Delivery Network. International Journal of Engineering and Advanced Technology (IJEAT) September 2019;Vol. 8, No. 6S3.
[57] Tetcos.com, ''NetSim-Network Simulator & Emulator | Home'', Available at: https://www.tetcos.com/,2019.
[58] D. Hadka, ''Beginner's Guide to the MOEA Framework'', 9781329825963, 2017.
[59] Hadeel S, Abbas Z, Hanan A. Hybrid DSR: Evaluating AODV-hello messages on DSR Protocol. Journal of Engineering and Applied Sciences 2019;14:4896–9.
[60] Park JH. Inner-product encryption under standard assumptions. Springer Designs, Codes, and Cryptography 2011;58(3):235–57.
[61] M. Scott, ''On the efficient implementation of pairing-based protocols''. Proceedings of 13th IMA International Conference IMACC, pp. 296-308, Oxford, UK: Springer Berlin Heidelberg, 2011.
[62] Martindale CR, Fotiadis G. Optimal TNFS-secure pairings on elliptic curves with even embedding degree. Cryptology ePrint archive; 2018/969, 2018..
[63] A. Guillevic. ''A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level''. PKC 2020 - IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, United Kingdom. pp.535-564, Jun 2020.
[64] M.A. TOURE, K. SAMAKE, S. TRAORE, ''Optimal Ate Pairing on Elliptic Curves with Embedding Degree 21'', International Journal of Science and Research (IJSR), https://www.ijsr.net/search_index_results_paperid.php?id=ART20203004, Vol. 8, No. 11, pp. 1659 – 1666, November 2019.
[65] Le D, Mrabet NE, Haloui S, et al. On the near prime-order MNT curves. AAECC 2019;30. doi: https://doi.org/10.1007/s00200-018-0363-1, pp. 107-125.
[66] Wang A, Guo B, Wei C. Highly-parallel hardware implementation of optimal ate pairing over Barreto-Naehrig curves. Integration Journal. 2019;64:13–21.
[67] Shortle JF, Thompson JM, Gross D, Harris CM. Simple Markovian Queueing Models. Fundamentals of Queueing Theory. 2020. doi: https://doi.org/10.1002/9781119453765.ch3.