[Egyptian Informatics Journal 22 (2021) 317–328](https://doi.org/10.1016/j.eij.2020.12.002)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/11108665)

Egyptian Informatics Journal

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

Full length article

[](http://crossmark.crossref.org/dialog/?doi=10.1016/j.eij.2020.12.002&domain=pdf)Efficient privacy-preservation scheme for securing urban P2P VANET networks

Bechir Alaya [⇑](#_bookmark0)

*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*

a r t i c l e i n f o

*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

a b s t r a c t

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 frame- work. 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 imple- mentation 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 eval- uation 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.

© 2021 THE AUTHOR. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelli-

gence, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creative-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[commons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

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]](#_bookmark15). Urban VANETs are highly mobile ad hoc wireless networks that have been implemented to provide passen- ger 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]](#_bookmark16).

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]](#_bookmark17). Several techniques for sensor networks [[5]](#_bookmark23),

topology, limited bandwidth, limited physical security, and energy use. Therefore, it is essential but difficult to design an effective sys- tem preserving the security and confidentiality of VANET networks.

Due to the mobility of the vehicle user, users can often commu- nicate with others on a VANET network or with the Peer-to-Peer (P2P) network exchange node [[10]](#_bookmark33). 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*VUi* ∈ *UP*2*PVANET*, let*Sim*(*VUi* ) the similar interests of *VUi*, and *Soc*(*VUi* ) represents the sociality of *VUi*, and defined as follows:

eHealth systems [[6 7]](#_bookmark26), vehicle communications [[8]](#_bookmark29), and intelligent

network communications [[9]](#_bookmark30) have been proposed. However, these

*Sim*(*VU* )= 1 *if VUi is sociable*;

# (1)

proposed schemes do not take into account the confidentiality of users of VANET networks and no longer take into account dynamic

*i*

0 *otherwise*.

When two users *VUi*, *VUj* ∈ *U* contact each other, the conditions necessary for establishing a social relationship based on the same similar interests are as follows:

\* Address at: MIS Department, College of Business and Economics, Qassim University, Al-Mulida Road, North Prince Nayef Airport, Qassim, KSA, Saudi Arabia.

*Soc*(*VUi*) = *Soc VUj* = 1, *VUi*, *VUj are sociables*; *Sim*(*VU* ) = *Sim* *VU* *have the same similar interests*.

# (2)

*i j*

(

*E-mail address:* [b.alaya@qu.edu.sa](mailto: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/© 2021 THE AUTHOR. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

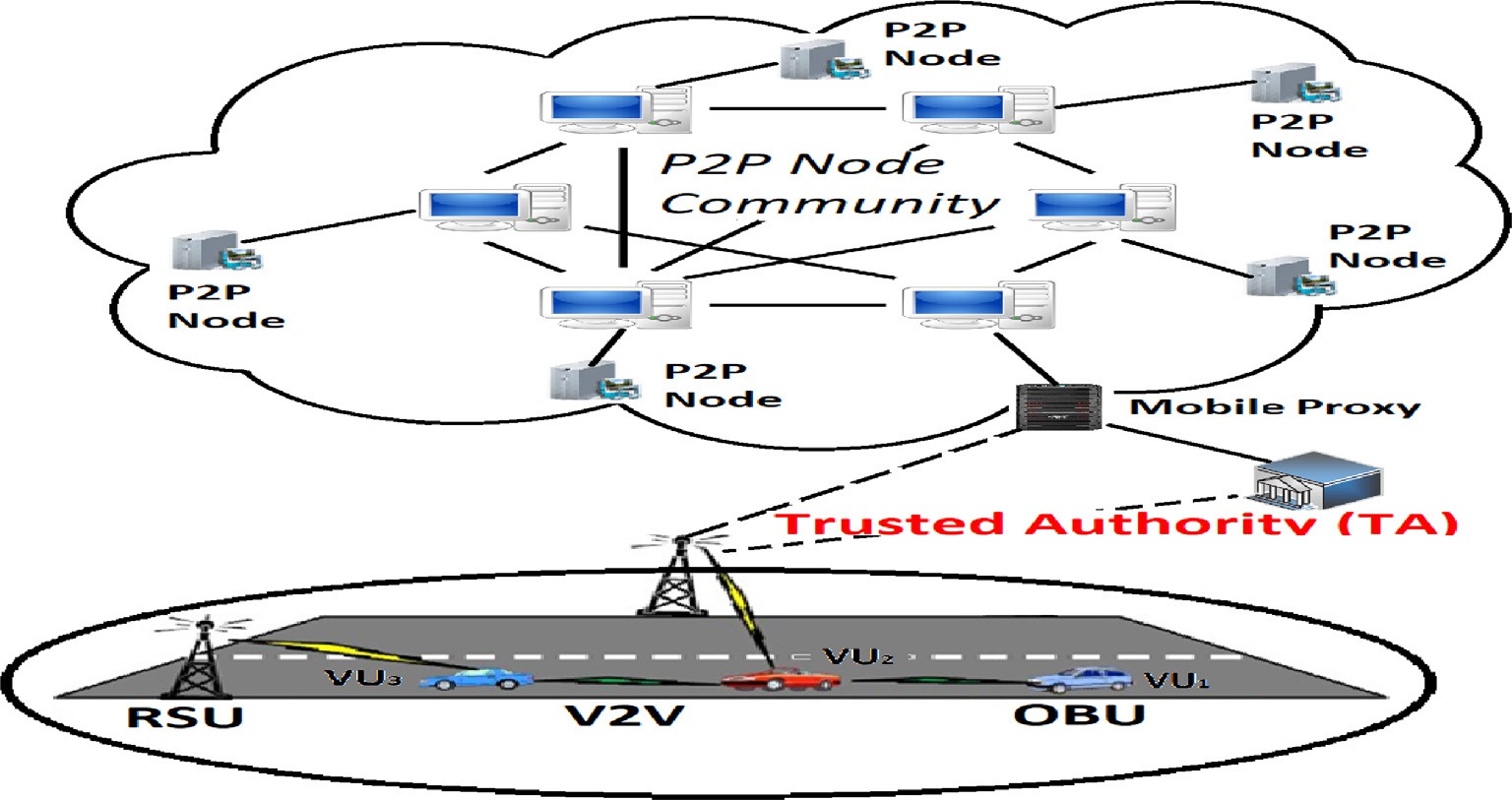


Fig. 1. The UP2PVANET system model.

In this work, the UP2PVANET network is considered, composed of a single TA (trusted authority), a large number of vehicle users VU = {VU, VU2, ·· ·, VU*n*} in an urban VANET network, and a P2P

node group, as shown in [Fig. 1](#_bookmark1). 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 *VUi* node the certificate and private key. Based on the proxy re-signature cryptography technol- ogy [[1112]](#_bookmark35), the node *VUi* can re-sign the certificate and can also verify the certificate.

To face security and performance problems, a secure and intel- ligent detection scheme is also introduced with a strong preserva- tion 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 ‘‘in- telligent” by adding new functions to understand their environ- ment 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 com- puter. Finally, to validate the security of our CSP2P scheme, the security properties of the proposed scheme are analyzing and sim- ulate it in two different scenarios. In the first scenario, the simula- tion results demonstrate that with a configuration of our proposed

diagram where the attack is launched on a certain number of

1. Review of related work

This section reviews the main existing work found in the scien- tific literature that applies video streaming over Peer to Peer Net- work and VANET.

* 1. *Video streaming over Peer to Peer*

P2P (Peer-to-Peer) network contributes to a large exchange of data of different types [[5]](#_bookmark23) 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]](#_bookmark37), 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]](#_bookmark39) by considering the core layer and cross-layer techniques in wireless networks and based on resilient techniques for P2P video streaming.

In [[15]](#_bookmark42) 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 specula- tion, a prefetching mechanism has been proposed to obtain a smooth reading, its mathematical model is as follows:

jumps, besides, more detections of black hole attack are presented. *P*

To achieve the practicality of our scheme, the performance of MP is

*rr*' =

{*k* |*k* } = *grr*' + *FIArr*' 3)

*r rr*'

(

*r r*' P *k* + *FIA*

also thoroughly assessed.

The rest of the article is organized as follows: [Section 2](#_bookmark2) high- lights the existing that applies video streaming over Peer to Peer Network and VANET network, and privacy-preservation and secu- rity schemes to the VANET network in the literature. [Section 3](#_bookmark3) describes the application of our CSP2P scheme video data replica- tion model and presents our replication algorithm. [Section 4](#_bookmark6), pre- sents a security analysis of the proposed CSP2P scheme. [Section 5](#_bookmark9) evaluates the solution based on simulation results analysis. Finally, [Section 6](#_bookmark13) concludes the paper and recommends many guidelines for future analysis.

Such as *Prr*' ,represents the association probability between the

node *r*and*r*' , *g* ' is the association between segment *kr* and seg- ment *kr*' , and *FIArr*' is the frequency increment from the association of segment *kr* to any other segment *kr*' .

*rr*

Evenly, a routing scheme for P2P live broadcast networks has

been proposed in [[16]](#_bookmark43). 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 com- munication due to the missed deadline or noise, and many others.

* 1. *Video streaming over VANET*

tance of the vehicle in the VANET, the authors proposed a multi- party security system with FHE.

VANET networks can treat vehicles as mobile detectors of the ~ 7

road situation in real-time [[1718]](#_bookmark45). In [[19]](#_bookmark46), the authors deal with live multimedia streaming in dynamic and loss VANETs using net-

The authors of [[32]](#_bookmark20) reduced the size of the public key to O(*k* )

based on FHE with integers, and later in other works they reduced

~ 5

work coding at the symbol level. Streaming data is disseminated

the size of the public key to O(*k* ), as in the case of [[33]](#_bookmark21). And to

~ ~

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]](#_bookmark35) 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 Mul- ticast 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 over- lay. 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]](#_bookmark48). 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 multi- path, and a strategy based on speculation prefect. In [[21]](#_bookmark18), 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]](#_bookmark18), 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 rout- ing protocols such as DSR (Dynamic Source Routing), and LAR (Location Aided Routing).

In [[23]](#_bookmark18) 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]](#_bookmark18), 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]](#_bookmark18), 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.

* 1. *Privacy-preservation and security schemes to the VANET network*

Many researchers aim to reduce the costs of attacks and secu- rity breaches in VANETs [[272829]](#_bookmark18). The use of homomorphic encryption is quite low in VANETs [[30]](#_bookmark18). A diagram relating to HE in VANET has been proposed in [[31]](#_bookmark19). They used an algorithm adopted on an algebraic circuit with a low multiplicative degree

reduce the asymptotic complexity from O(n2.5) to O(n1.5), the authors of [[34]](#_bookmark22) introduced a fully homomorphic scheme with priming functionality. In [[35]](#_bookmark24) they deciphered the messages and they reduced the overload by using FHE with a p006Flylog of size

~

O(*k*) and depth (*k*).

In [[36]](#_bookmark25), the authors used the public key homomorphism prop- erty. On the other hand, in [[37]](#_bookmark27), They proposed a scheme with a computational complexity of kA^ · 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]](#_bookmark28), threshold FHEs with the monotonic Boolean formula [[39]](#_bookmark31), diagram, algebraic FFEs with multivariate polynomials [[40]](#_bookmark32), and FHEs with sorting on encrypted data without decryption [[4142]](#_bookmark34). Wang et al. have used FHE in [[43]](#_bookmark36) with reduced time for encryption, decryption, and re-encryption with Fast Fourier Transform. In [[44]](#_bookmark38), challenges on integers have been implemented with a simple FHE to optimize complexity. Fan et al. have proposed an algorithm [[45]](#_bookmark40) 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]](#_bookmark41).

* 1. *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.

1. 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

~ 3.5

of probabilistic decryption. The complexity was a bit readyO(*k* ) knowing that *k* represents a security parameter. In [[31]](#_bookmark19), another scheme was proposed to avoid the estimation based on the dis-

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]](#_bookmark51) |  | MNT-80 [[65]](#_bookmark51) |  | BN-128[[66]](#_bookmark51) |  |
| G2  *k* | F*e*  2 |  | F*e*3  6 |  | F*e*  12 |  |
| Modulus (bits) | 512 |  | 160 |  | 256 |  |
| Paring curve type | Tate [[62]](#_bookmark51) |  | Ate [[64]](#_bookmark51) |  | Tate [[62]](#_bookmark51) |  |
| 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 |

* 1. *Homomorphic encryption and identity-based signature*
     1. *Homomorphic encryption*

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

A *KeyGen* key generation algorithm takes as input a security parameter 1*k* 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 mes- sage *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, ·· ·, *En*) relating to the messages (*m*1, *m*2, ·· ·, *mn*) respectively. It returns an encrypted *E* = *Enc*(*K*, *Pky*, *C*(*m*1, *m*2, ·· ·, *mn*)).

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* : G1 × G2 → G*Z* having

three properties, i.e., computable, bilinear, and nondegenerate as detailed in [[48]](#_bookmark44).

In our work, the public key in HE is (M, *f* ), and the correspond-

ing private key is (*a*, *b*). Let *E*(·) 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* · *xMmodM*2 (4)

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

*E*(*m*1) · *E*(*m*2) = *f m*1 · *x*1*M* *f m*2 · *x*2*M* *modM*2

= *f m*1 +*m*2 · (*x*1*x*2)*MmodM*2 (5)

= *E*(*m*1 + *m*2)

Also, hash chains [[4950]](#_bookmark47) are used that are one-way functions.

* + 1. *Signature-based on identity*

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

Key generation: either *Ui* is the user identity, the *Gpk* calculates

*.Ui* = *CH*1(*Ui*)∈ G1 and the associated private key

*Apk* = *mk* · *.Ui* ∈ G1 that is transmitted to the user.

Signature: to sign a message, the user chooses a random num- ber *r* ∈ Z\*, and calculates *X* = *r* · *T*, *Y* = *Apk* + *r* · *CH*2(*Ui*, *M*, *X*). The signature on *M* will be the couple *l* =< *X*, *Y* >.

*k*

Verification: To verify the signature *l* =< *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*)).

* 1. *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]](#_bookmark49). Two control messages are initialized by each node VU = {VU, VU2, ·· ·} of UP2PVANET, such as *{MesDem, MesRes}*. These messages have the format of the ‘‘RREQ route request” message [[52]](#_bookmark50). Such that each message consists of three

parts, the general communication costs, the verification costs, and the signature costs (see [Table 1](#_bookmark4)). Either the bilinear parameters (*k*, *T*, G1, G2, 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 *Encsy*(.), and three secure hash functions *CH*1, *CH*2, *andCH*3, where *CH*1 : {0, 1}\* → G1, *CH*2 : {0, 1}\* →

G2, *CH*3 : G*Z* → Z\*. Also, the TA chooses a random number

*k*

*x* in Z\*, and calculates *T* = *x* · *TandCTA* = *x* · *CH*1(*UiTA*), Such as *UiTA* represents the identity chain of the TA.

*k*

1. According to the confidentiality requirements of most nodes, the TA chooses D*e* and defines the certificate validity period of D*e*. Then, and according to the density of the MP: in each

domain, the TA decides the certificates that must update from an MP.

1. TA calculates the corresponding private key (*a*, *b*), and the

public key of the Homomorphic encryption (M, *f* ).

1. TA keeps the master key (*a*, *b*, *mk*, *CTA*, *x*) as secret, and shares the system parameters in UP2PVANET:
2. *Ppub* = {*k*, *T*, G1, G2, G*Z* , *e*, *T*, *CH*1, *CH*2, *CH*3, *M*, *f* , *Encsy*(.), D*e*}
3. When *MPi*(*i* = 1, ··· , *n*) registers in the system, TA calculates the private key based on identity *SKMPi* = *xCH*1(*IDTA * *IDMPi* ), where *IDTA*is the identity chain of TA, *IDMPi* is the identity chain of *MPi*, and *SK* represents the session key which is semantically secure [[53]](#_bookmark50), and which serves as a necessary condition for the confidentiality of the receiver session.

Then, the TA sends *SKMP* to *MPi* via a secure channel.

*i*

Config: The private key generator (*Gpk*) first chose two groups

G1*and*G2 of the first-order *k* > 2*k* with *k* is the security parameter. Then *Gpk* chooses the generator *T* of G1 and the random master key *mk* ∈ Z\* and calculates the associated public key *pk* = *mk* · *T*. It also takes on the cryptographic hash functions *CH*1, *CH*2 : {0, 1}\* → G1\*.

*k*

The public system parameters are (*k*, G1, G2, *e*, *CH*1, *CH*2).

* 1. *Key and certificate sent by MP*

When a new vehicle node *VUi* wishes to communicate with other vehicle nodes in the domain *Clj*, the *MPi* delivers the private

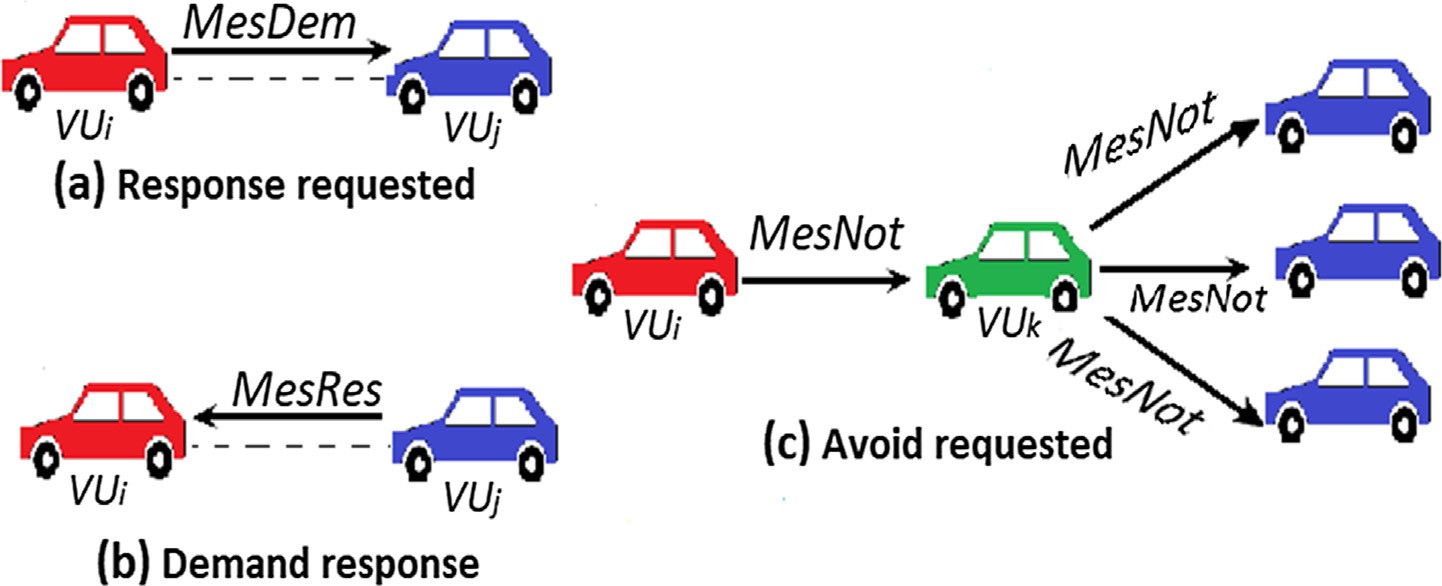


Fig. 2. Detection scheme based on neighbor × neighbor cooperation.

key *SKVUi* and the certificate *CertMPi* ,*VUi* as shown in the following list :

1. The *MPi* chooses a random number *xMP* in Z\* as the master
2. According to the certificate *CertMPi* ,*VUj* it decides that the link with node *VUj* is proven if *CertMPi* ,*VUj* is valid. Else, it decides that the link with node *VUj* is not proven.

*i k*

key, and calculates the pseudo-identity

*PIVUi* = *EncxMP* (*IDVUi* ), the private key

Algorithm. 1: The requested response algorithm

*i*

*SKVUi* = *xMPi CH*1(*IDMPi * *PIVUi* ), and the public key

*pkVU* = *xMPi T*, where *IDVUi* is the identity chain of *VUi* and

*Input: Current timestamp &MesDem*

* 1. *Select a random number xVU* in Z\*

*i i k*

*IDMPi* is the identity chain of *MPi*. Then the *MPi* calculates his private point *TMPi* = *xMPi T* and *TMPi* = *xCH*1(*IDMPi* ).

* 1. *Calculates: Cp that represents ciphertext of*

*MesDem* -

*VU*

1. *MP*

generates the certificate *Cert*

< *pk*

, *R* >, with

*Cp* = *E*(*MesDem*) = *f MesDem* · *x*

*VUj modVU*2

*Such*

*i MPi* ,*VUi*

*VUi*

*VUi*

*VUi*

*VUj*

*R* = *PIVU* + *xMP CH*2(*IDMP* , *SKVU* , *PIVU* ).

*aspkVUj* < *f VUj* , *VUVUj* >

1. *MP*

*i i* *i*

*SK Cert*

*i* *i*

*VU* via a secure channel.

1. *for each VUj* ∈ 1 — *hopofVUido*

*i* sent

*VUi* and

*MPi* ,*VUi* to *i*

1. *Select the shortest time between two messages (s*)
   1. *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](#_bookmark5)).

* + 1. *The requested response*

Adversary node can send false messages by creating private

1. *Send\_Request* (*Cp*, *VUj*)
2. *EndOutput: The ciphertextCp*

Algorithm. 2: The demand verification algorithm

*Input: The ciphertext C*

1. *When the node VUi receive the ciphertext C*
2. *Recover MesRes from the ciphertext C*

*VUj*

communication tunnels., i.e., black hole attack. However, each node *VUi* ∈ *UP*2*PVANET* runs Algorithm. 1 to initiates a response

1. *MesRes* =

*L* *CamodVU*2

· *bmodVU*

*VUi*

request for nodes *VUi*, and to execute the notification phase it waits

1. *Where SKVU* < *a*, *b* > *from MesRes*

for the response to its request. This phase is summarized by the

following steps:

1. *Recover Cert*

*i*

*MPi* ,*VUj*

*from MesRes*

* 1. The node *VUi* signs the message *MesDem*with the public key *pkVUj* < *f VUj* , *VUVUj* > of the receiving node *VUj* and the ran- dom number *xVUj* in Z . (See Algorithm.1)

*k*

\*

* 1. *VUj* 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.
  2. After having received a message from *VUj* node, *VUi* extracts the response message MesResencrypted from *Cl*. Then the node *VUi* extracts *CertMPi* ,*VUj* from MesRes and checks the validity of the certificate with *MPi* (See Algorithm 2).

1. *Checks the certificate CertMPi* ,*VUj with MPi*
2. *If CertMPi* ,*VUj is not valid then*
3. *return not proved*
4. *else*
5. *return proved*

*Output: proven or not proven link*

* + - 1. *Response to the request.* As the requested attack detection response, *VUj* decides to execute the Algorithm. 3 when it receives the detection request. This phase of response to the request is rep- resented as follows:
         1. *VUj* node recovers *CertMPi* ,*VUi* from *MesDem* and validates the certificate with *MPi* (See Algorithm. 3).
         2. CSP2P scheme executes the Algorithm. 1. in the case of the certificate *CertMP* ,*VU* is not valid. In the other case, *VUj* signs

Algorithm. 4: The avoid\_requested algorithm

*i j*

the message *MesRes* with *pkVUi* < *f VUi* , *VUVUi* >of the trans- mitter node *VUi* and the random number *xVUi* in Z .

*k*

\*

* + - * 1. The node *VUj* waits for the time of requested attack detec- tion response to run out and sends the encrypted text *D*. (See Algorithm 3, lines 12 to 13)

*Input: MesNot, and VUi*

1. *If (VUi* ∈ (1 — *hopofVUx)) then*
2. *Remove VUifrom the routing table of VUx*
3. *Select xVU* (*thatrepresentsarandomnumber*) in Z\*

*i k*

1. *for each VUz* ∈ 1 — *hopofVUx do*
2. *calculate E the ciphertext of MesNot*
3. *E* = *E*(*MesNot*) = *f MesNot* · *xVUVUz modVU*2

*VUz*

*VUx*

*VUj*

Algorithm. 3: The Request-Response algorithm

*Input: The control message MesRes, the ciphertext C, and VUi*

* 1. *When the node VUi receive the ciphertext C*
  2. *Recover MesRes from the ciphertext C*

*VUj*

1. *Where pkVUi* < *f VUz* , *VUVUz* >
2. *Select the shortest time between two messages*
3. *Send\_Request*(*E*, *VUz*)

*Output: The ciphertextE*

1. *MesRes* =

*L* *CamodVU*2

· *bmodVU*

*VUj*

- Once the CSP2P scheme is successful, *VUi* and *VUj* nodes can

1. *Where SKVU* < *a*, *b* >

give mutual support to other neighbors, and also can share

1. *Recover Cert*

*i*

*MPi* ,*VU*

*from MesDem*

experiences and information safely, using the evolution of the certificate. Thanks to these promising features, UP2PVANET

1. *Checks the certificate CertMPi* ,*VUi with MPi*
2. *If CertMP* ,*VU is not valid then*

can be widely used by multiple vehicle users. Besides, as shown

1. *i i* in the Algorithm. 5, because the Access Point (AP) is not always

requested response (.)

1. *else*
2. *Select a random number xVUj*
3. *Calculates: Cp that*

in Z\*

*ciphertext of*

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

*MesRes* -

*k*

*represents*

(multimedia data, textual data, etc.).

*Cp* = *E*(*MesRes*) = *f MesRes* · *xVUVUi modVU*2

*Such*

*VUi*

*aspkVUi* < *f VUi* , *VUVUi* >

*VUj*

*VUi*

1. *Select the shortest time between two messages (s*')
2. *Send\_Request* (*Cp*, *VUi*)
3. *End*

*Output: The ciphertextCp*

* 1. *Evolution of the certificate*

The identity chain *ID* to *ID * *t* is only valid before the specified expiration date *t* for a *VUi* node. After the expiration of *t*, if a new certificate is not generated by *MPi*, the corresponding certifi- cate *CertMPi* ,*VUi * *t* is revoked. For this, CSP2P uses proxy re- signature cryptography technology [[54]](#_bookmark50), to adopt an efficient recovery strategy.

* *VUi* removes the adversary node *VUx* in its 1-hop routing table, in the case where *VUi*decides that the link with the *VUx*is unpro- ven. As shown in the [Fig. 2](#_bookmark5) (c), *VUi* sends complaints to all its neighbors. When the neighbor node receives the claim (notifi- cation request), then it removes *VUx*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. 5: Collaborative Information algorithm

*Input: status of AP*

* 1. *Vehicle user VUiperiodically collect information Infi*
  2. *If an AP is nearby available, then*
  3. *VUi immediately select Inf to P2P Node group*
  4. *else if a Vehicle User VUi is nearby then*

* 1. *if (soc*(*VUi*) = *soc VUj* &&*sim*(*VUi*) = *sim VUj ) then*
  2. *VUiandVUjexchange their data*
  3. *Before Infi’s expiration: VUi helps Infi when it encoun- ters available access points; else, deletingInfi*
  4. *End if*
  5. *End if*

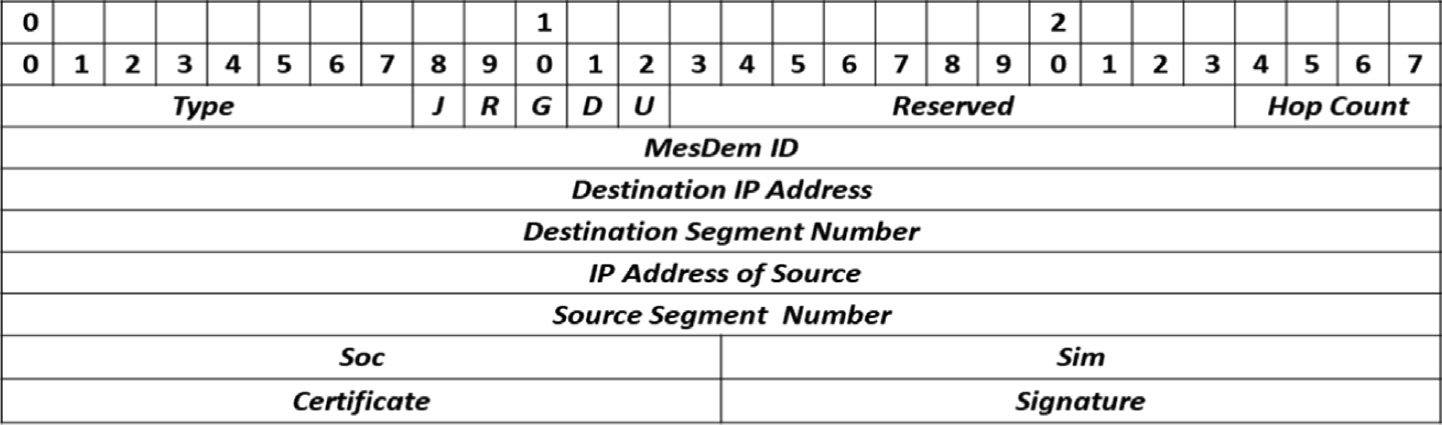
*Output: Information Infi*

1. 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”.



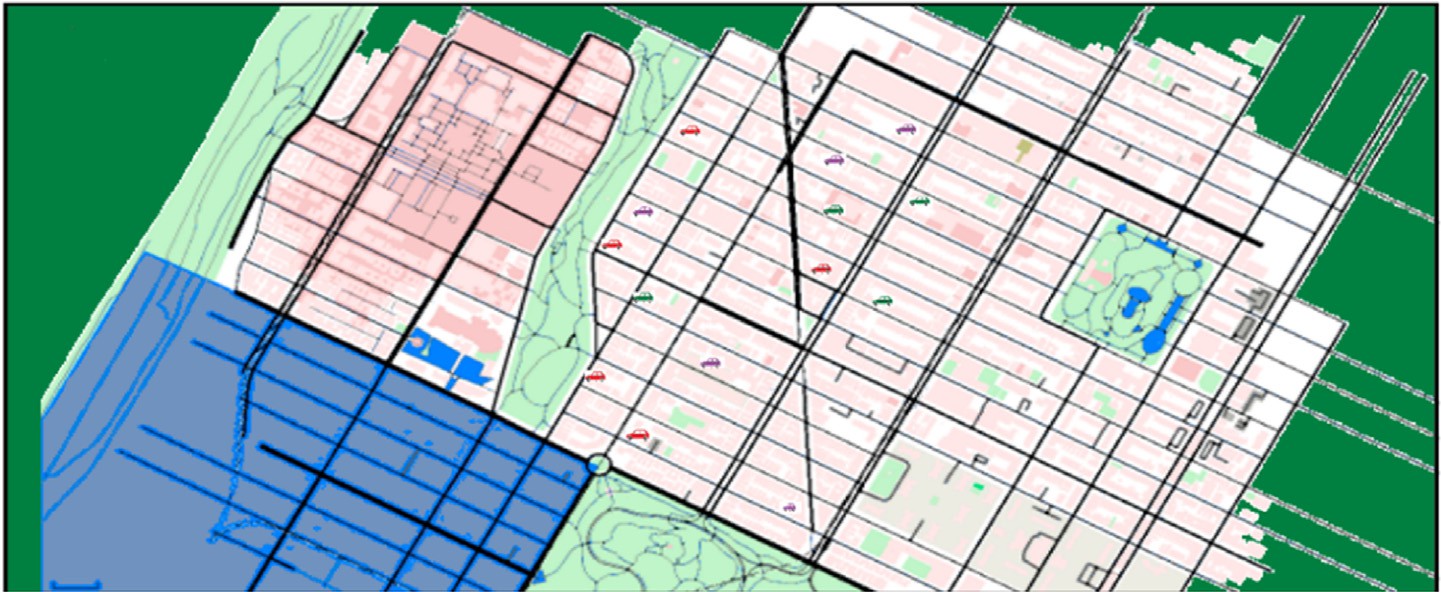


Fig. 3. Topology Urban VANET network from SUMO.

on how the CSP2P scheme will follow to ensure message confiden- tiality [Table 2](#_bookmark7).

* 1. *Semantic security of CSP2P scheme*

Let a polynomial opponent *P* that try to take advantage of knowledge from the challenger *CH*. According to the CSP2P scheme, *P* could follow the following rules: *1)* R.Not(Sk*pub*, *e*)

which permit *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 *e* selected by *P*; *2)* R.Mod(S, q, *L*)which is used by *P* to change the *message-signature (S, q)* with the *L* changes he wishes. The rule

resend a valid and modified signature if the modifications are admissible on the error; *3)* R.Prove(*S*, q, *W*)permit *P* to obtain a justification of the origin *message-signature (S, q)* depending to *W*{(m*x*, q*x*)}*x*∈[1.k] (database). *4)* R.Not/Mod*a*(S, *e*, M) permit *P* to assume as input S, e, and M. If *a* = 1, it modifies the original signa-

'

ture of the message S by M. Otherwise if *a* = 0, it resends *S* as a message which corresponds to the message modified by M.

* 1. *Confidentiality preservation*

In CSP2P, it is a control messages based on homomorphic encryption [[55]](#_bookmark50), such as *{MesDem, MesRes}*. Even if *P* spies on the encrypted text, he can never sign the corresponding message. *P*cannot get the message across, even if *P* compromises the *MPi* database. Consequently, CSP2P guarantees confidentiality preservation.

* 1. *Certificates evolution*

In this phase, even if *P* is spying on the exchange between

*MP andVU* , he cannot get the certificate information. Otherwise,

tion 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 cov- erage 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 (*ttd*). [Fig. 3](#_bookmark8) shows the transport map of a metropolitan region exported from OSM.

* 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 × 500*mto*1500 × 1500*m* depending on the size of the UP2PVA- NET 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 (SI1) and the group of form *g*1, and the other half

have the same interests (SI2) and the group of form *g*2. Each node

randomly selects a destination in the region using the shortest

route and with speed *d*. Moreover, let *R*2 the maximum transmis- sion range. Let also, *P*n,Ne,Ad that indicates the probability that it exists at least n neighboring nodes in *pR*2 (the transmission range) of an adversary of surface *Sr*.

# *P*n,Ne,Ad = *P* N ≥ n|*pR*2

= 1 — *P* N < n|*pR*2

*n*—1

*i i* = 1 — X *P* N = *i*|*pR*2 (6)

even if *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

*i*=0

X*n*—1 |*d*| *pR*2 *i*

= 1 —

· 1 —

*i*=0

*i*

*Sr*

*pR*2 |*d*|—*i*

*Sr*

The simulation of the CSP2P scheme for the security and confi-

dentiality of UP2PVANET is carried out via the NetSim version 10 simulator [[56 57]](#_bookmark50) and the MOEA framework [[58]](#_bookmark50) to optimize the

Let *Dbh* be the black-hole detection rate, which is expressed as follows:

# 1

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

*Dbh* = 

*D*

*t*

Such as *tD*

represents the time of the attack detection.

(7)

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 optimiza-

Let *sr* be the social report of a group *g* with, *sr* = *ThenumberofsociableVU*

by supposing that the two SI1*and*SI2 have the interest report*sr* = [0.3, 0.4, 0.5, 0.6].

*allVUing*

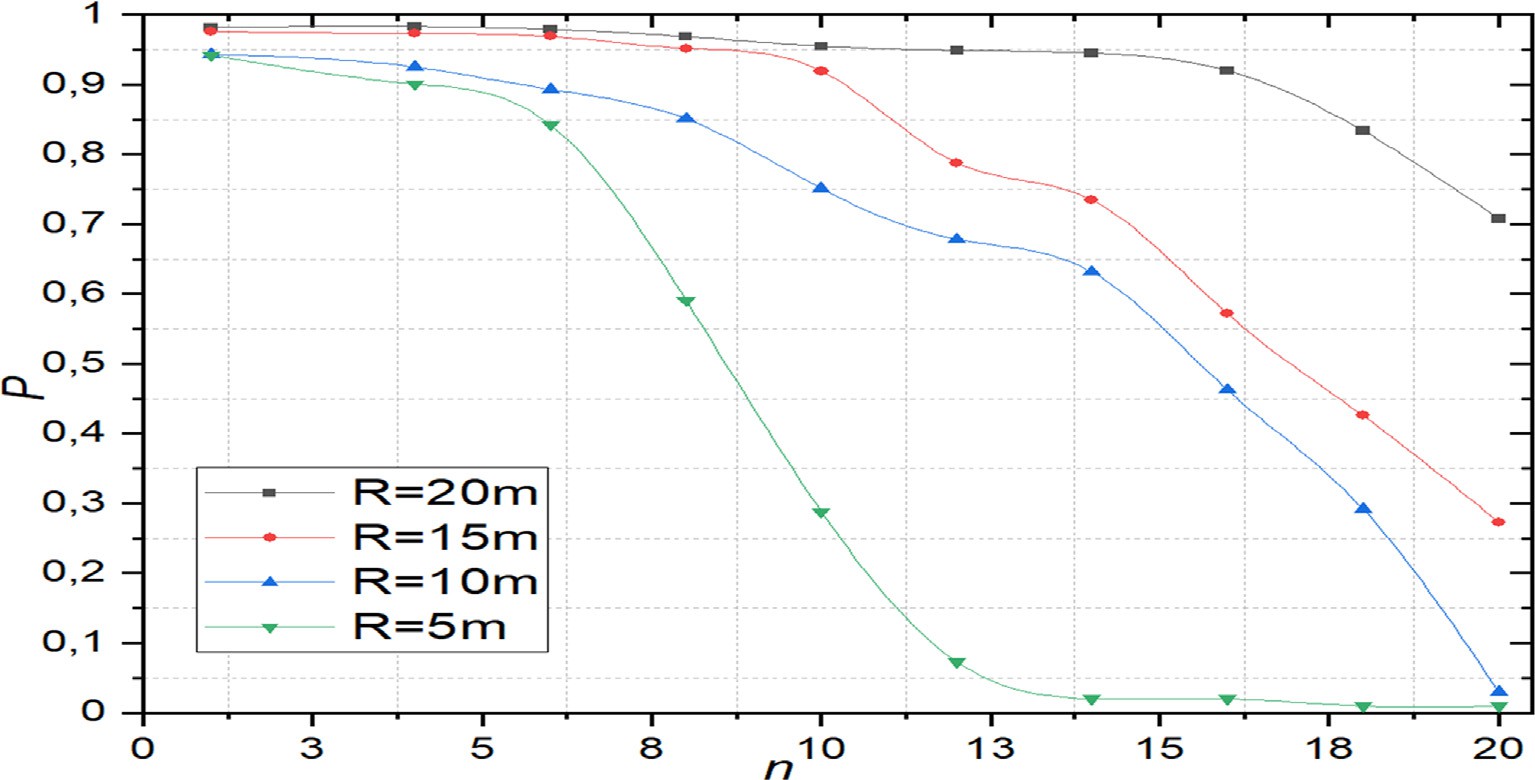


Fig. 4. The probability of *n* neighbors of an adversary *P*n,Ne,Ad.

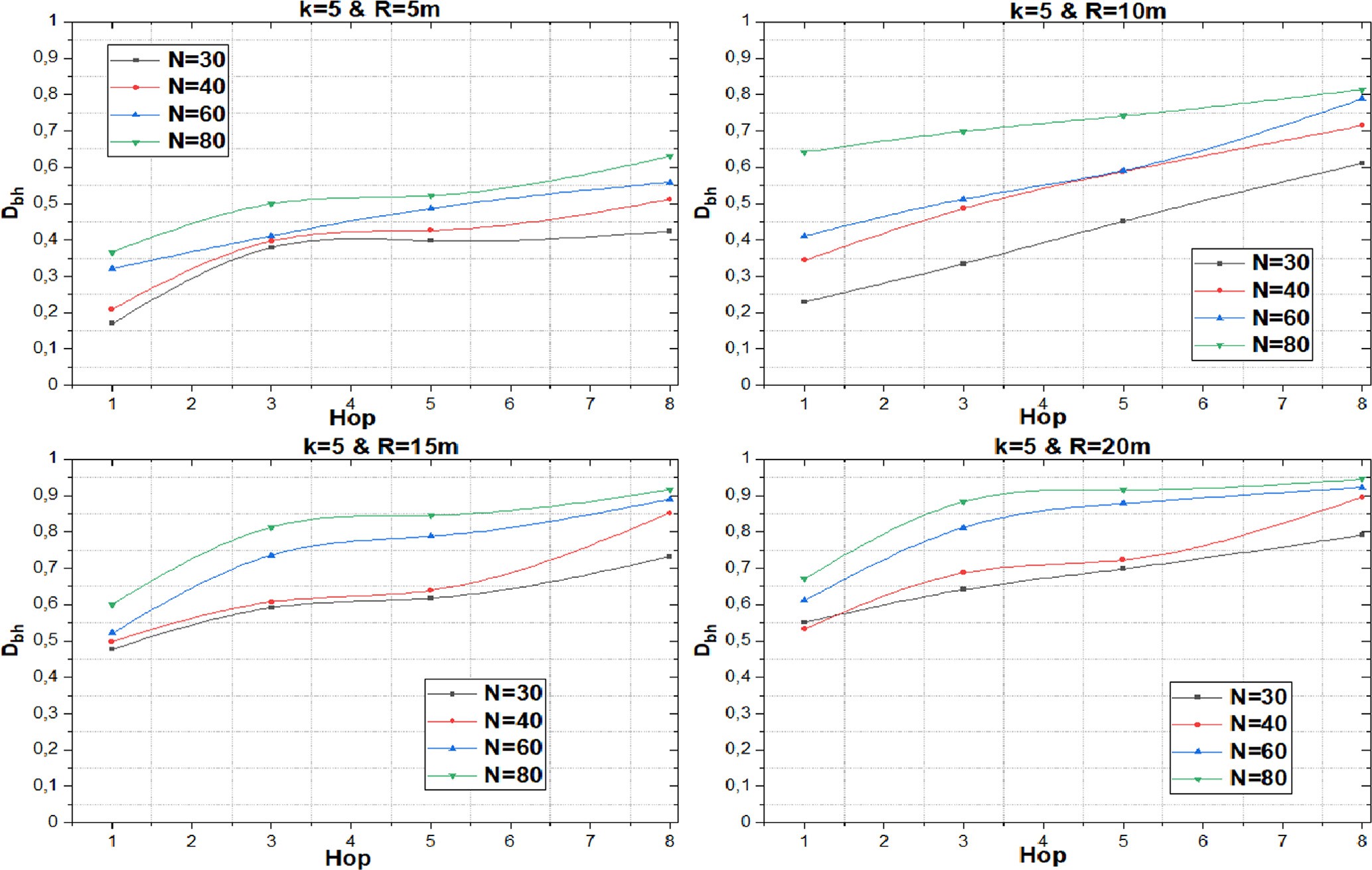


Fig. 5. Blackhole bond detection rate *Dbh* varying with the Hop (tunnel length).

[Fig. 4](#_bookmark10) presents the probability of *n* neighbors of *P*n,Ne,Ad in a UP2PVANET network, with different values of *n*, (1 ≤ *n* ≤ 20). With *n* ≤ 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](#_bookmark11) illustrates the rate of detection of the black hole *Dbh* vary- ing according to the length of the tunnel (Hop) which represents the interval of jumps between the adversaries, where:

*R* ∈ [5, 10, 15, 20]*andn* = 5. As shown in [Fig. 5](#_bookmark11), *Dbh* increases with

increasing *R* throughout the UP2PVANET network. When the attack is launched over several additional hops, note that *Dbh* is

more detected. Also, from the same figure, note also that *Dbh*will increase considerably with the increase of *N*.

[Fig. 6](#_bookmark12) presents *Dbh* varying according to *Hello transmission pro- tocol* [[59]](#_bookmark50) (*HTP* ) to discover the neighbors and check periodically the presence of neighbors, and the different durations of the black hole attack, such that *R* ∈ [5m, 10m, 15m, 20m]*andn* = 5. [Fig. 6](#_bookmark12) shows if the detection rate of the black hole is longer than its attack

duration. Also, [Fig. 6](#_bookmark12) show that the detection rate of *Dbh* increases in the whole UP2PVANET network, with an increase of *R*. CSP2P takes longer to detect if the transmission interval *HTP*is long

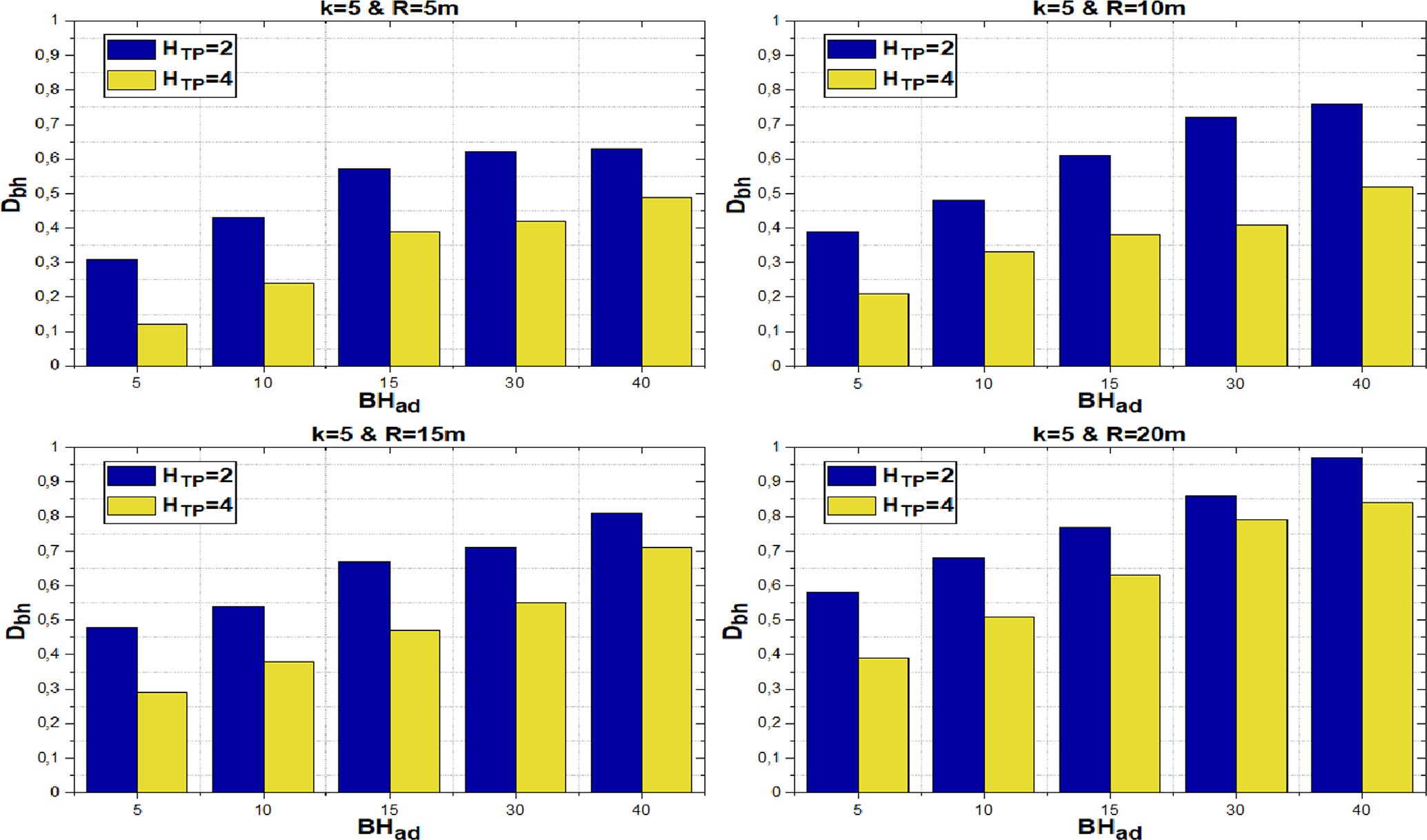


Fig. 6. Blackhole bond detection rate *Dbh* varying with the *Hello transmission* (*HTP* ) and black hole attack duration *BHad*.

enough. Therefore, the use of small message transmission intervals

*tv* = 1 · 2 — *b* , with*b* = *k*

# (8)

is more efficient for the CSP2P scheme.

* 1. *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 met- ric 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 Z\* en- crypt, decrypt, hashing operations, and authentication. The results of the measurements are given in the [Table 1](#_bookmark4). The homomorphic encryption of the predicates is adopted to internal products (IPE) [[60]](#_bookmark50), and the numbers obtained in the [Table 1](#_bookmark4) [[61]](#_bookmark51), to estimate the cost calculation in CSP2P.

*t*,

Tate pairing curve type [[62]](#_bookmark51) is used, with the integration degree

*k* = 2 Cocks-Pinch (CP-80) [[63]](#_bookmark51). CP-80 is on F*e* with 512 bits of the

* + 1. 2 — 2*b l*

The black hole attack results in a transmission delay. Also, the encryption and decryption operations cause the transmis- sion 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 *ithMesDem* in the node to

wait for the arrival of the next(*i* + 1)*thMesDem*. When a valid *Mes- Dem* message is buffered at the node, then many *MesDem authen- tications* at the node level are presents, that represents a geometrically distributed random variable:

# P(*k*) = *pk*—1(1 — *p*) (9)

Specifying *tw* as the average waiting time, as follows:

∞

*k*=1 *l*

*l*(1 — *p*)

first-order *e*. Next, using the Ate paring curve type [[64]](#_bookmark51) with a

degree of integration *k* = 6Miyaji-Nakabayashi-Akano (MNT-80)

*tw* = X *k* · *pk*—1(1 — *p*) = 1

# (10)

[[65]](#_bookmark51). MNT-80 is on F*e*3 with 160 bit of the first-order *e*. Finally,

using the Tate pairing curve type [[62]](#_bookmark51) with the integration degree *k* = 12 Barreto-Naehrig (BN-128) [[66]](#_bookmark51). BN-128 is on F*e* with 256 bits of the first-order *e*.

With *w* = 1, 2, ··· , *m* — 1. In the case of *w* = *m* ⇒ *tw* = *tm* = 0 Therefore, before sending the message *MesDem*, a waiting time of each *MesDem* in the node buffer is presents that will be:

The Poisson Input, Constant Service, Multiserver (M/D/1) [[67]](#_bookmark51) process are implemented to evaluate the transmission delay in our CSCNET scheme. Considering the starting rate *l*, the average

*Tj* =

*m*—*j*

(1—*p*)

( *l*

, *j* = 1.2, ·· ·, *m* — 1;

0, *j* = *m*

# (11)

arrival *MesDem* at the node level follows a Poisson process with

The average waiting time is as flows:

an arrival rate *k*, and advancing the process from state*i* to *i* + 1. The time *MesDem* average delay before being put into the node buffer is *tv* , which is as follows:

*Tj* =

*m*—*j*

(1—*p*)

( *l*

, *j* = 1.2, ·· ·, *m* — 1;

0, *j* = *m*

# (12)

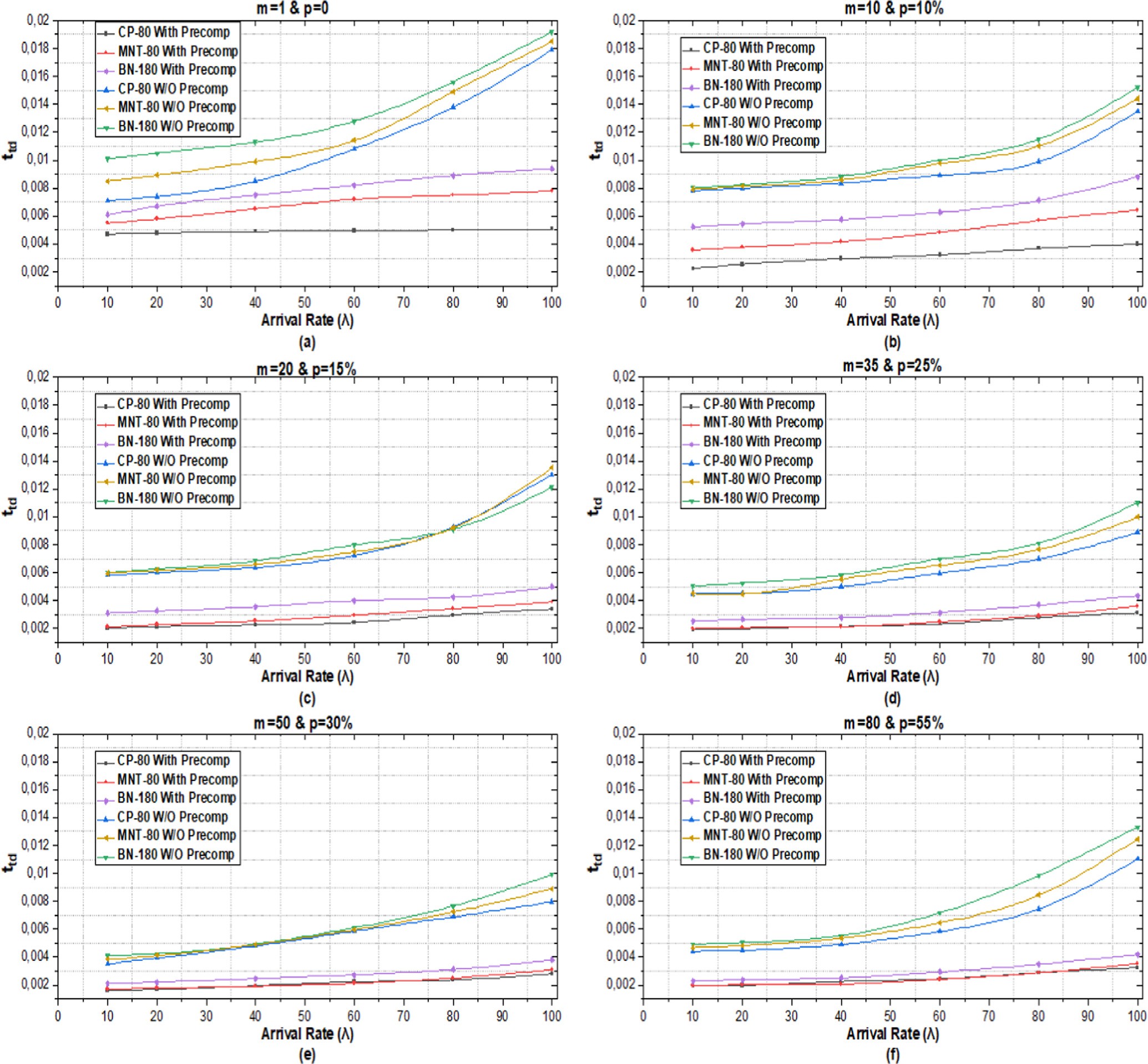


Fig. 7. Transmission delay *ttd* vs arrival rate *k*.

The average waiting time is as flows:

# *tw* = X 1 · *Tj* = 1 · 1 · (1 + 2 +· ··+ (*m* — 1))

m

the parameters of *m* and from *p*. As shown in the [Fig. 7](#_bookmark14) (a,b,c,d,e,f), overall *ttd* increases with the increase of *k*. Also, the transmission delay *ttd* with the Miyaji-Nakabayashi-Takano curve (MNT-80)

*j*=1 *m*

* + 1. *l*(1 — *p*)

and the Barreto-Naehrig curve (BN-128) is greater than the Cocks-Pinch curve (CP-80). Furthermore, [Fig. 7](#_bookmark14). roughly shows

1 1 *m*(*m* — 1)

the relationship between *ttd* and *p*, *m*, such that the transmission

= *m* · *l*(1 — *p*) ·

1 *m*(*m* — 1)

# 2 (13)

*m* — 1

delay *ttd* will also increase with the increase of *pandm*. Concluding also that with a more improved performance of a node, the trans- mission delay of *CP-80* can be considerably optimized.

= *m* · 2*l*(1 — *p*) = 2*l*(1 — *p*)

Consequently, concluding that the transmission delay *ttd* from our CSCNET scheme to the node at the receiver is as follows:

*ttd* = *tv* + *tw* + *td* = 2 — *b* + *m* — 1 + *td* (14)

2*l* 1 2*l* 1 *p*

# ( — *b*) ( — )

[Fig. 7](#_bookmark14). represent the average of the transmission delay *ttd* vary- ing with *k* of Poisson’s process, where 1 ≤ *k* ≤ 100, and also fixing

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 net- work. CSP2P can not only meet the security and confidentiality requirements of the UP2PVANET network but can also detect, pre- vent, and inform elementary and compound attacks. The results of

the theoretical and experimental analyses illustrate the effective- ness of our CSP2P scheme. This fact is confirmed by the reduction of delays for the VANET network and convergence towards a per- manent 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 finan- cial 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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0005) [Network and Vehicle Cloud Computing: A Survey. Wireless Communications](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0005) [and Mobile Computing 2020;31:1–25](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0005).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0015) [survey. IEEE Commun Mag 2013;51(5):148–57](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0015).
4. [More S, Naik UL. ‘‘Optimization driven Multipath Routing for the video](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0020) [transmission in the VANET,”](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0020) [IEEE Global Conference on Wireless Computing](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0020) [and Networking (GCWCN). India: Lonavala; 2018. p. 6–10](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0020).
5. [Lu R, Lin X, Zhu H, Liang X, Shen X. BECAN: a bandwidth-efficient cooperative](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0025) [authentication scheme for filtering injected false data in wireless sensor](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0025) [networks. IEEE Trans Parallel Distrib Syst 2012;23(1):32–43](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0025).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0035) [(security and privacy) in wireless body area networks for healthcare](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0035) [applications. Egyptian Informatics Journal 2017;18(2):113–22](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0035).
8. [Liang X, Li X, Luan T, Lu R, Lin X, Shen X. Morality-driven data forwarding with](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0040) [privacy preservation in mobile social networks. IEEE Trans Veh Technol](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0040) [2012;61(7):3209–21](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0040).
9. [Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy- preserving](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0045) [aggregation scheme for secure smart grid communications. IEEE Trans Parallel](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0045) [Distrib Syst 2012;23(9):1621–31](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0045).
10. [Yang L, Li H. Vehicle-to-vehicle communication based on a peer-to-peer](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0050) [network with graph theory and consensus algorithm. IET Intel Transport Syst](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0050) [2019;13(2):280–5](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0050).
11. [Ling HY, Wang K. Dynamic overlay multicast for live multimedia streaming in](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0055) [urban VANETs. Comput Netw 2012;56(16):3609–28](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0055).
12. [Xiaoliang W, Jianming J, Shujing Z, Liang B. A Fair Blind Signature Scheme to](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0060) [Revoke Malicious Vehicles in VANETs. Computers, Materials & Continua](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0060) [2019;58(1):249–62](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0060).
13. [Masinde N, Graffi K. Peer-to-Peer-Based Social Networks: A Comprehensive](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0065) [Survey. SN Computer Science 2020;299:1–51](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0065).
14. [Abboud O, Pussep K, Kovacevic A, Mohr K, Kaune S, Steinmetz R. Enabling](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0070) [resilient P2P video streaming: survey and analysis. Multimedia Syst](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0070) [2011;17:177–97](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0070).
15. [Xu C, Zhao F, Guan J, Zhang H, Muntean G-M. QoE-driven user-centric VoD](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0075) [services in urban multihomed P2P-based vehicular networks. IEEE Trans Veh](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0075) [Technol 2013;62:2273–89](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0075).
16. [Ayatollahi H, Khansari M, Rabiee H. A push-pull network coding protocol for](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0080) [live peer-to-peer streaming. Computer Network 2018;130:145–55](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0080).
17. [Hu M, Zhong Z, Ni M, Wang Z, Xie W, Qiao X. Integrity-oriented Content](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0085) [Offloading in Vehicular Sensor Network. IEEE Access 2017;5:4140–53](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0085).
18. [Zhangjie F, Lili X, Yuling L, Zuwei T. Privacy-Preserving Content-Aware Search](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0090) [Based on Two-Level Index. Computers, Materials & Continua 2019;59](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0090) [(2):473–91](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0090).
19. [Zhenyu Y, Ming L, Lou W. CodePlay: Live Multimedia Streaming in VANETs](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0095) [Using Symbol-Level Network Coding. Wireless Communications, IEEE](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0095) [Transactions on August 2012;11(8):3006–13](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0095).
20. [Xu C, Zhao F, Guan J, Zhang H, Muntean GM. QoE-Driven User-Centric VoD](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0100) [Services in Urban Multihomed P2P-Based Vehicular Networks. Vehicular](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0100) [Technology, IEEE Transactions on Jun 2013;62(5):2273–89](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0100).
21. [Jung HC et al. ‘‘An adaptive multimedia streaming dissemination system for](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0105) [vehicular networks. Applied Soft Computing‘‘ 2013;13(12):4508–18](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0105).
22. [Yang X, Liu J, Zhao F. A vehicle-to-vehicle communication protocol for](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0110) [cooperative collision warning. Boston, MA, USA: IEEE Mobiquitous; 2004. p.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0110) [114–23](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0110).
23. [Xu S, Guo P, Xu B, Zhou H. QoS evaluation of VANET routing protocols. Journal](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0115) [of Networks 2013;8:132](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0115).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0125) [vehicular networks. Int J Distrib Sens Netw 2013;9:309041](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0125).
26. [Cao D, Yuchen J, Jin W, Baofeng J, Osama A, Amr T, et al. ARNS: Adaptive Relay-](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0130) [Node Selection Method for Message Broadcasting in the Internet of Vehicles.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0130) [Sensors 2020;20(5):1–18](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0130).
27. [Tyagi P, Dembla D. Performance analysis and implementation of proposed](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0135) [mechanism for detection and prevention of security attacks in routing](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0135) [protocols of vehicular ad-hoc network (VANET). Egyptian Informatics Journal](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0135) [2017;18(2):133–9](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0135).
28. [Zhihua X, Lihua L, Tong Q, Jae SH, Xianyi C, Byeungwoo J. A Privacy-Preserving](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0140) [Image Retrieval Based on AC-Coefficients and Color Histograms in Cloud](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0140) [Environment. Computers, Materials & Continua 2019;58(1):27–43](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0140).
29. [Al Abdulkarim A, Al-Rodhaan M, Tian Y, Al-Dhelaan A. A Privacy-Preserving](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0145) [Algorithm for Clinical Decision-Support Systems Using Random Forest.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0145) [Computers, Materials & Continua 2019;58(3):585–601](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0145).
30. [Wenbo S, Jiaqi W, Jinxiu Z, YuPeng W, Dongmin C. A Novel Privacy-Preserving](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0150) [Multi-Attribute Reverse Auction Scheme with Bidder Anonymity Using Multi-](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0150) [Server Homomorphic Computation. Intelligent Automation and Soft](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0150) [Computing 2019;25(1):171–81](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0150).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0160) [scheme in opportunistic VANETs. Security and Communication Networks](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0160) [2016;9(15):2789–801](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0160).
33. [Coron JS, Mandal A, Naccache D, Tibouchi M. Fully Homomorphic Encryption](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0165) [over the Integers with Shorter Public Keys. Crypto 2011;6841:487–504](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0165).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0175) [Scheme. EUROCRYPT 2011;6632:129–48](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0175).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0185) [key homomorphic encryption, arithmetic circuit ABE and compact garbled](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0185) [circuits. Berlin, Heidelberg: Springer; 2014. p. 533–56](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0185).
38. [Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0190) [(standard) LWE. SIAM J Comput 2014;43(2):831–71](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0190).
39. [Canetti R, Raghuraman S, Richelson S, Vaikuntanathan V. Chosen-Ciphertext](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0195) [Secure Fully Homomorphic Encryption. In: IACR International Workshop on](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0195) [Public Key Cryptography. Berlin, Heidelberg: Springer; 2017. p. 213–40](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0195).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0210) [Search Over Encrypted Data for IoT with Privacy-Preserving, Computers.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0210) [Materials & Continua 2019;60(2):675–90](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0210).
43. [Kogos KG, Filippova KS, Epishkina AV. Fully homomorphic encryption](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0215) [schemes: The state of the art. In: In Young Researchers in Electrical and](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0215) [Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian. p. 463–6](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0215).
44. [Wang W, Hu Y, Chen L, Huang X, Sunar B. Exploring the feasibility of fully](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0220) [homomorphic encryption. IEEE Trans Comput 2015;64(3):698–706](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0220).
45. [Chen Y, Nguyen PQ. Faster Algorithms for Approximate Common Divisors:](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0225) [Breaking Fully-Homomorphic-Encryption Challenges over the Integers.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0225) [EUROCRYPT 2012;7237:502–19](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0225).
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.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0235) [LogEvent2vec: LogEvent-to-Vector based Anomaly Detection for Large-Scale](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0235) [Logs in Internet of Things. Sensors 2020;20(9):2451](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0235).
48. [Fau S, Sirdey R, Fontaine C, Aguilar-Melchor C, Gogniat G. Towards practical](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0240) [program execution over fully homomorphic encryption schemes. P2P, Parallel,](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0240) [Grid, Cloud and Internet Computing (3PGCIC), Eighth International Conference](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0240) [2013:284–90](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0240).
49. [Yu Z, Yin L, Yifan W. Secure and Efficient Searchable Public Key Encryption for](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0245) [Resource Constrained Environment Based on Pairings under Prime Order](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0245) [Group. Security and Communication Networks. 2019;2019:1–14](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0245).
50. [Krawczyk H, Rabin T. Chameleon signatures. NDSS 2000. USA: California;](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0250) [2000. http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/042.pdf](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0250).
51. [Agarwal P. Secure Node Communication With Cryptographic Algorithm in](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0255) [Vehicular Ad Hoc Networks. International Journal of Advanced Science and](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0255) [Technology 2017;109:1–12](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0255).
52. [Asit D, Martin K, Dinkar S. Dynamic Segment Replication Policy for Load-](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0260) [Balancing in Video-on-Demand Servers. IEEE Multimedia 1994;3(10):1–24](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0260).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0280) [Content Delivery Network. International Journal of Engineering and Advanced](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0280) [Technology (IJEAT) September 2019;Vol. 8, No. 6S3](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0280).
57. Tetcos.com, ‘‘NetSim-Network Simulator & Emulator | Home”, Available at: [https://www.tetcos.com/,2019.](http://www.tetcos.com/%2C2019)
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0295) [DSR Protocol. Journal of Engineering and Applied Sciences 2019;14:4896–9](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0295).
60. [Park JH. Inner-product encryption under standard assumptions. Springer](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0300) [Designs, Codes, and Cryptography 2011;58(3):235–57](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0300).
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](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0310) [with even embedding degree. Cryptology ePrint archive; 2018/969, 2018.](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0310).
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?](http://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](https://doi.org/10.1007/s00200-018-0363-1%2Cpp.107-125).
66. [Wang A, Guo B, Wei C. Highly-parallel hardware implementation of optimal](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0330) [ate pairing over Barreto-Naehrig curves. Integration Journal. 2019;64:13–21](http://refhub.elsevier.com/S1110-8665(20)30161-4/h0330).
67. Shortle JF, Thompson JM, Gross D, Harris CM. Simple Markovian Queueing Models. Fundamentals of Queueing Theory. 2020. doi: [https://doi.org/10.1002/](https://doi.org/10.1002/9781119453765.ch3) [9781119453765.ch3](https://doi.org/10.1002/9781119453765.ch3).