Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 1615015, 15 pages
https://doi.org/10.1155/2021/1615015

Research Article

Named Data Networking-Based On-Demand Secure Vehicle-To-Vehicle Communications

Qudsia Saleem,[1] **Ikram Ud Din**,[1] **Ahmad Almogren**,[2] **Ibrahim Alkhalifa**,[2] **Hasan Ali Khattak**,[3] **and Joel J. P. C. Rodrigues**[4,5]

[1]*Department of Information Technology, The University of Haripur, Pakistan*
[2]*Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia*
[3]*School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan*
[4]*Senac Faculty of Ceará, 60160-194 Fortaleza CE, Brazil*
[5]*Instituto de Telecomunicações, Portugal*

Correspondence should be addressed to Ikram Ud Din; ikramuddin205@yahoo.com, Ahmad Almogren; ahalmogren@ksu.edu.sa, and Hasan Ali Khattak; hasan.alikhattak@seecs.edu.pk

Received 16 September 2021; Revised 22 October 2021; Accepted 30 October 2021; Published 26 November 2021

Academic Editor: Shalli Rani

The detection of secure vehicles for content placement in vehicle to vehicle (V2V) communications makes a challenging situation for a well-organized dynamic nature of vehicular ad hoc networks (VANET). With the increase in the demand of efficient and adoptable content delivery, information-centric networking (ICN) can be a promising solution for the future needs of the network. ICN provides a direct retrieval of content through its unique name, which is independent of locations. It also performs better in content retrieval with its in-network caching and named-based routing capabilities. Since vehicles are mobile devices, it is very crucial to select a caching node, which is secure and reliable. The security of data is quite important in the vehicular named data networking (VNDN) environment due to its vital importance in saving the life of drivers and pedestrians. To overcome the issue of security and reduce network load in addition to detect a malicious activity, we define a blockchain-based distributive trust model to achieve security, trust, and privacy of the communicating entities in VNDN, named secure vehicle communication caching (SVC-caching) mechanism for the placement of on-demand data. The proposed trust management mechanism is decentralized in nature, which is used to select a trustworthy node for cluster-based V2V communications in the VNDN environment. The SVC-caching strategy is simulated in the NS-2 simulator. The results are evaluated based on one-hop count, delivery ratio, cache hit ratio, and malicious node detection. The results demonstrate that the proposed technique improves the performance based on the selected parameters.

1. Introduction

Transmissions nowadays become necessary among devices, communication servers, and more specifically among vehicles [1]. Vehicle communication leads us towards the new type of network called vehicular ad hoc network (VANET). VANET is a special type of network in which one vehicle communicates with other vehicles and roadside communications towers. This network contains two types of nodes, i.e., roadside units (RSU) and on-board units (OBU). Vehicles are moving objects, and the installed equipment is fixed on roadsides [2]. Communications in VANETs take place in three categories, i.e., vehicle-to-roadside infrastructure (V2I), vehicle-to-vehicle (V2V), and infrastructure-to-infrastructure (I2I) communications. The communication is possible through the installed wireless communications infrastructures. Multiple RSUs are installed on roadsides, which may effectively provide access to content inside vehicular communications infrastructures. A single base station (BS) that controls the entire communications is possible inside and outside the communication infrastructure. The infrastructure-based communication is only possible when everything is in the control of RSU and BS. The proposed framework only considers communications between vehicles, i.e., V2V communications. The basic concept is to provide communications among vehicles in a secure communication environment. VANET enhances road safety, reduces traffic congestion, and controls traffic information sharing. In addition to all this information, VANET can provide weather information and multimedia content.

Traditional IP-based VANET communications make the quality of service (QoS) task more complex on the provision of the services. On the other hand, VANET can provide benefits in terms of safety applications. Information-centric networking (ICN) converts content requests from host-centric networking to content-centric networking [3], where all requests are handled based on the content names rather than communication channels. The proposed framework uses content-based instead of IP-based communications, which make the system more secure for infrastructure-based communications. Various architectures have been proposed, where named data networking (NDN) has gained higher popularity due to its most effective communication features in terms of security [4], reliability, and efficiency [2]. Typically, NDN contains three data structures, i.e., forward information base (FIB), pending interest table (PIT), and content store (CS) [5].

This research was conducted based on VNDN secure communications among vehicles. Content is stored on selected vehicles that can handle requests of other vehicles inside the communication range. The CS caches content coming from RSUs without any security policy. The PIT stores the incoming interfaces and pending requests from vehicles. Another responsibility of the PIT is to create back link paths from one hop to another inside the request tables. Finally, the FIB maps the content with the attached prefixes to arrange content requests of the vehicles. Figure 1 shows the data exchange in the ICN-based VANET communications. The NDN routers are fixed, whereas in the VNDN, the routers are vehicles with high mobility [5, 6]. Since there is no mobility support in NDN, it results in a frequent data retrieval failure [7].

The cluster-based network architecture can enhance the network performance by reducing the number of vehicles involved in the forwarding. Thus, it enhances network stability [6, 8]. However, the selection of clusters and cluster head (CH) in VANETs is challenging due to trust management issues. In the highly dynamic nature of VANETs, the selection of CH is a critical issue. The problem found in this approach is the detection of compromised requests coming from malicious nodes. Besides, some malicious vehicles transfer wrong information, compromise the VANET trustable environment, and alter the messages broadcast in the V2V environment, which can cause serious traffic accidents and some other critical issues in the VNDN. To improve the security in VANETs, several schemes have been proposed in the literature. However, these techniques are not sure to provide the current V2V security in the on-demand environment. Since users in the vehicular environment do not know each other, there should be a mechanism that can provide trust and secure communications among the participating vehicles to avoid miss behaviors. Here, centralized trust management does not provide better solution due to communication delay [9]. Therefore, a distributed trust mechanism is needed for secure VANET communications.

In the proposed solution, the blockchain mechanism is used for secure V2V communications. The SVC-caching strategy has been introduced to cache content in the VNDN environment. The SVC-caching provides a secure placement of NDN content on vehicles after the selection of a CH. The content may be traffic information and popular data with a high dynamic nature. The proposed strategy is aimed at providing a secure environment for the selection of the cache node and content placement. The SVC-caching can also detect malicious requests received from infected vehicles. The main contributions of this study are listed below:

(1) proposes a novel strategy for blockchain-based trustable V2V communications in a highly dynamic vehicular environment

(2) selects cluster nodes and CH using a customized K-Means dynamic clustering algorithm

(3) presents a strategy to place content using an NDN approach for intervehicle communications in clusters

(4) provides secure V2V communications for reliable and stable content placement, where vehicles request entertainment better than other VANET caching placement strategies

The rest of the paper is organized as follows. Section 2 reviews the previous researches. Section 3 presents the proposed SVC-caching strategy, clustering transformation, and a secure placement of NDN content. Research evaluation and discussion on results are presented in Section 4. The presentation of the feasibility of the SVC-caching and its contributions are presented in Section 5. At last, the conclusion and future directions are presented in Section 6.

2. Literature Review

Various strategies have been proposed by the research community for solving security issues in content caching and sharing [10, 11]. Each strategy has its own advantages and limitations. The existing techniques designed for caching and security of data in the VANET environment are discussed here in detail.

In [5], the idea of ICN was proposed wherein the leave copy everywhere (LCE) was supposed to be deployed. LCE is a reactive caching strategy that cache content on all on-path nodes lies between the publisher and subscribers. The beauty of this strategy is such that if a content is accessed once, its copy would be available for all future requests. Therefore, the content delay is reduced, and the cache hit ratio is increased. However, the availability of content on all nodes increases redundancy, which may fill the node cache soon, and the new arriving content would not have space to be stored. In the remaining of the paper, LCE will be referred to as *reactive caching*.

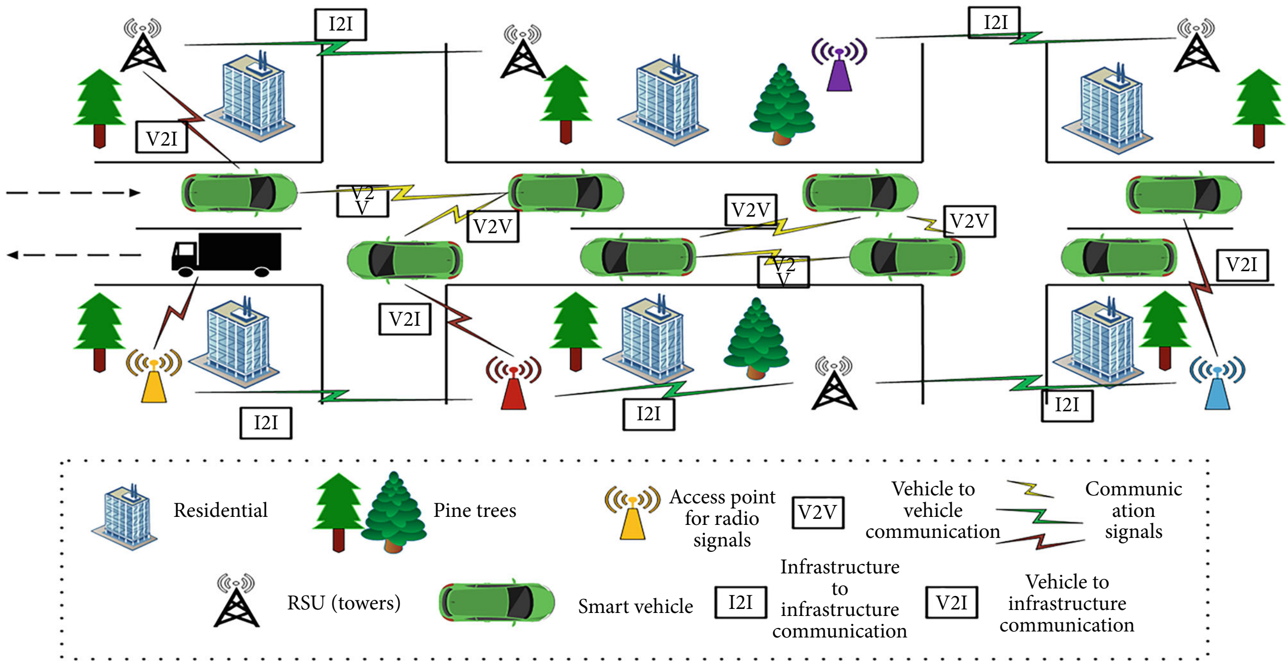
I2I
I2I
V2I
V2V
V2V
V2V
V2V
V2V
V2I
V2I
V2I
I2I
I2I
I2I
Residential
Pine trees
Access point for radio signals
V2V
Vehicle to vehicle communication
Communication signals
RSU (towers)
Smart vehicle
I2I
Infrastructure to infrastructure communication
V2I
Vehicle to infrastructure communication

Figure 1: Communications in the VANET environment.

In [12], the authors identify that the current host-centric vehicular model does not support the new device registration and handling capabilities in a large number. Their scheme, named PeRCeIVE, is proposed for mobile node delivery problems. PeRCeIVE is a proactive caching approach for data placement at right network elements. A hierarchical namespace is used to name the address for each chunk of the data packet. The first algorithm calculates the chunk lists for requested data, and the second one examines the chunk distribution. The simulation results show that the PeRCeIVE approach improves the one-hope ratio and resolves interest ratios in a limited/average number of cached copies inside the network with a comparable threshold. However, this approach seems to be unsuitable for large cache sizes because it is better for a limited number of content cached in a node's cache.

In [13], a content name-based addressing mechanism, named neighbor cache explore routing based on trajectory prediction (PNCE), is proposed that works efficiently in a dynamic VANET environment. Due to dynamic and weak network connections among vehicles, it is important to adopt a routing protocol for message broadcasting in an emergency situation. With the use of an in-centering cache strategy, the proposed mechanism works well for reducing redundant packet traffic and choosing an optimal path for forwarding information. The PNCE claims to improve the round-trip delivery ratio. However, periodically broadcasting beacon messages may cause packet congestion in a network.

With the intention of settling in to VANET scenarios, a few routing protocols are determined by geographical locations in the VND environment. For instance, name/ID-based routing protocol (we will call it IR protocol throughout the article) [14] judges the next hop by measuring the path between the publisher and subscribers. The main theme is to get to the destination with a minimum number of hops. Nevertheless, the IR protocol seems to be imprecise because of the mobility option. Moreover, IR may not be deployed in the VNDN since it does not support the in-network caching capabilities in addition to caching unnecessary content on the path [13].

In [15], the authors proposed a group leader and group members' strategy for secure V2V communications. In the proposed methodology, a secure connection is established between the group leader and member vehicles in a network by broadcasting asymmetric keys to all member vehicles, whereas the message is encrypted with a symmetric key. To manage overlapping vehicles in a network, the authors proposed a multihop communication mechanism. Moreover, for the authentication of vehicles, the group-based hybrid model is utilized and malicious vehicles are detected by comparing the trust score to a threshold value. Based on the network of vehicles, the paper also discusses the revocation process, which reduces the certificate revocation list (CRL) size and increases the network performance. For evaluation, the scheme combines direct trust calculation and feedback from neighbor vehicles. The proposed mechanism achieves successful results for trust management. However, there are maximum chances of content retrieval delay because of encryption and decryption of keys at each node.

Security credential management system (SCMS) is presented in [16]. This system is in the transition phase and develops a dynamic identifier (ID) virtualization method. Moreover, the method makes difficult for attackers to generate valid messages in addition to preventing controller area network (CAN) logs from being analyzed. In [17], a secure caching mechanism is proposed for VNDN wherein the reputation of nodes is calculated using a blockchain mechanism to achieve privacy and security. In the NDN environment, each node serves as a cache store, forwarder, and consumer of the data at the same time. Therefore, there should be a mechanism that can protect the cache content in the VNDN, which is based on three roles, i.e., forwarder, consumer, and content store. The authors propose the reputation-based trust mechanism to calculate the trustworthiness of the cache store in order to make the communications secure and reliable. This is achieved by taking the experience of consumers to give the reputation value to the content store, i.e., intermediate node on data consumption that provides the requested content. The requested content is stored in the blockchain network based on the validation of the content by consumers. The reputation of each content is updated after validating it from the blockchain. The same mechanism will be followed for the content that will be received by consumers. If the reputation is greater than the threshold value, then the data will be consumed. In case of false data received, the consumer will issue a new interest for the same content. The consumer will create a new block to send the reputation value to the blockchain network. The results are compared with the normal NDN approach, which shows that the proposed mechanism stores zero nontrusted content irrespective of the caching policy. However, due to generation of new requests for the same content in the case of false data received, the redundancy is increased.

A blockchain-based IoT system is developed in [18, 19] wherein IoT nodes store the private key, whereas the Ethereum public keys are stored to perform data provenance in the IoT network. Many algorithms are presented for IoT ecosystems, which can be studied in [20, 21]. However, there are only few solely blockchain-based algorithms. The authors in [22] deliberate the challenges related to electric vehicles (EVs) and present a registration and authorization mechanism for various scenarios. The presented model is a decentralized security model, which is smart contract and lightning network in the blockchain ecosystem.

In [23], the authors propose a solution for secure message dissemination in VANET using blockchain technology. In addition, the authors assume that the vehicle is a full node having the capabilities to mine new blocks and the normal node helps in the message verification and forwarding process. The RSUs and vehicles use asymmetric keys and digital signature technology for the validation and verification process. The miner will be able to mine the block if it solves the proof-of-work puzzle and gets a nonce value, which is generated periodically according to the difficulty target of the vehicle. The authors check the validity of critical messages through blockchain, which are not encrypted and have local region of interest (ROI). The validity of the message is verified by at least 15 vehicles on the basis of proof-of-location. The mining vehicle will validate the message and calculate the new trust value of the vehicle's broadcasting message. The location certificate is issued by RSU with a time stamp, which makes the verification process more trustworthy [24]. The session ID will be assigned to the vehicle. The vehicle will send back its session ID signed with a digital signature. If the vehicle response is less than the threshold time, then, the certificate will be issued to the vehicle; otherwise, it may be rejected. The proof-of-location check will prevent the denial-of-service, spamming, or other hassle attacks. The simulation shows that the proposed solution works well for trusted emergency message dissemination in the VANET environment. However, several certificates may be rejected if the vehicle response is less than the threshold time.

In [13], on the basis of cache and geographical parameters, a mechanism, named neighbor cache explore routing based on trajectory prediction (PNCE), is proposed. Vehicles are categorized as providers, containing the actual content of data, and consumer vehicles that request the data. Moreover, the packets are divided into three categories, namely, beacon packets, interest packets, and data packets. A forwarding model that contains four components, i.e., CS, FIB, neighbor table (NT), and neighbor cache table (NCT), is proposed. The actual content is stored in the CS, whereas the FIB table contains the record of the reverse path and each entry has three associated fields, i.e., node ID, next hop ID, and timestamp. Geographical location's information is cached in the NT, and neighbor's cached content is stored in the NCT. Moreover, the NT is updated on the basis of timestamp and NCT is updated on the basis of content cached in neighbor's node. To access information from an unknown destination for the first time, the interest packets are broadcast until the provider sends the requested data to consumers. Each vehicle upon receiving the interest packet either delivers the requested data or calculates the next hop in the network, whereas the FIB table is utilized to finding the closest source by using the distance prediction method. With the use of an in-centering cache strategy, the proposed mechanism works efficiently for reducing redundant packet traffic and choosing an optimal path for forwarding information. However, the response latency may increase because of the interest packet broadcast in the network until the consumer receives the data sent by the publisher.

In [25], a cluster-based cooperative caching approach is introduced with the prediction mechanism of the mobility of vehicles in VNDN. The proposed clustering algorithm groups similar mobility pattern vehicles within the same cluster through a prediction technique. After grouping, the cooperative caching technique based on intercluster and intraclustering communications for clusters is applied. Furthermore, the most popular caching data and least popular caching data are handled separately based on the frequency of access rates. At the end, multiple cache placement and cache transmission schemes are proposed for VNDN. The proposed strategy has the advantage of enhancing cache and network performance for communications. However, the performance degrades for different types of vehicles and large cache sizes. In [26], a secure trust model for autonomous vehicles is proposed for the authentication of information and protection of vehicle tracking in VNDN. The proposed model contains four entities, i.e., autonomous vehicle organization, manufacturer, vehicle, and data. A hierarchical naming for the key generation process is adopted. The manufacturer assigns a unique vehicular ID to all vehicles when manufactured. The trust anchor in this approach is the autonomous vehicle authority who validates the data by a unique ID assigned to the manufacturer. The technique stops false data dissemination in the network.

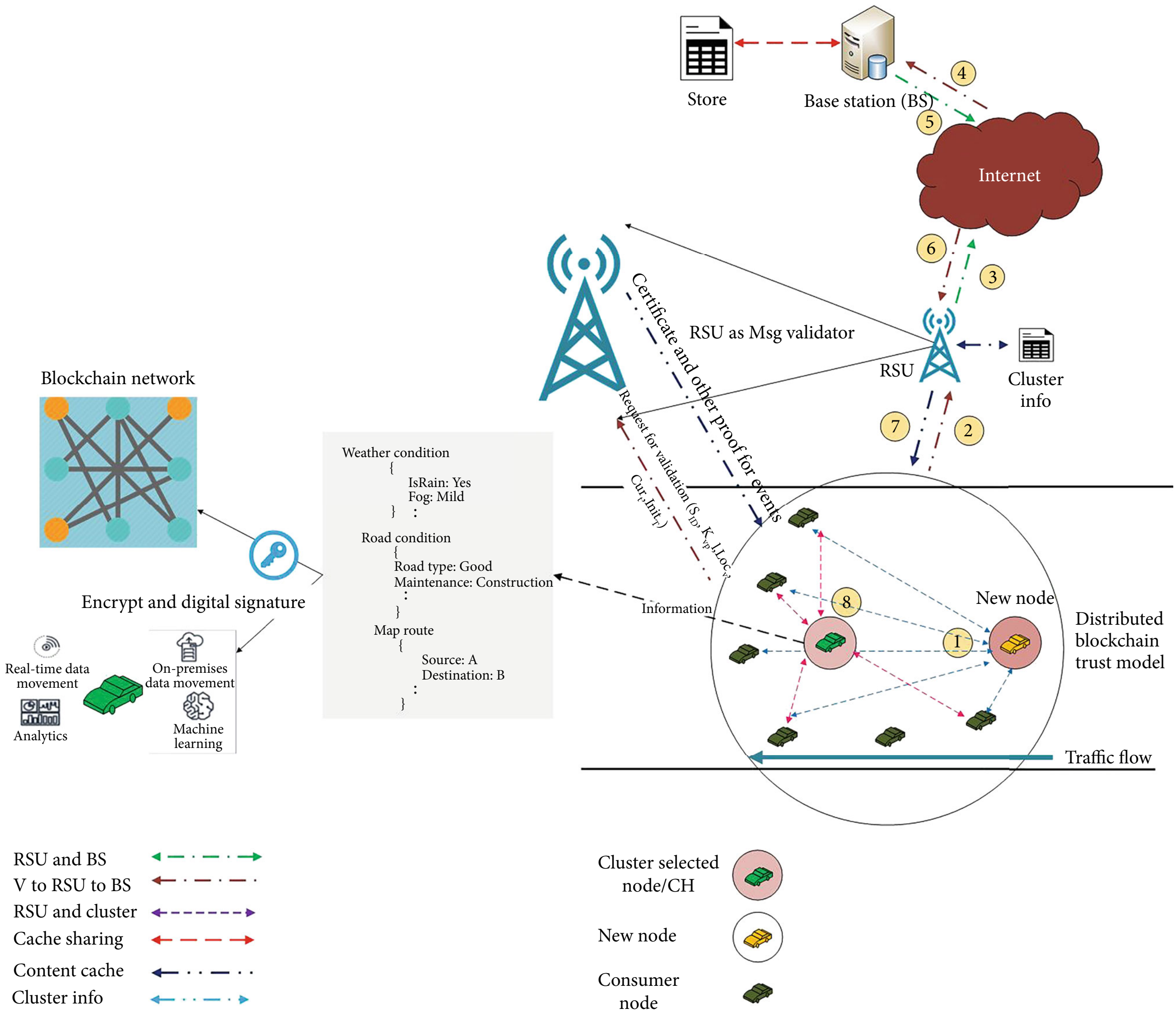

Figure 2: Architecture of the blockchain-based VNDN.

```
Steps:
        1. Start
        2. $V_{PreviousT} \longleftarrow V_{NDNB}$
        3.
if ($RSU_{POL} \longleftarrow$issue()) then
                $V_{RSUSessID} \longleftarrow$ TRUE
                $T_{Vres} \longleftarrow$ Threshold
                add-message()
                else
                reject-message()
4. End
```

Algorithm 1: Message verification policy (MVP) adopted by each normal node.

The second contribution is the protection of vehicle tracking, which is achieved by introducing a pseudonym instead of the vehicle ID, which is used in the certification process and hides the actual identity of the vehicle. However, this approach may increase content retrieval delay due to checking the certificates for several times for the content validity.

In [27], a mechanism is proposed to detect various kinds of attacks and the attack table is updated to record the

```
Steps:
        1. Start
        2. Nonce-value-check() ⟵ Bi
        3. N⟵ $(H(M_i)\|H(B_i - 1)\|N)$
        4. check-trust()⟵ (check(LOC)
        && check-time()&& $M_{IDsg}$)
        5. check($N < D_t$)
        6.
if ($M_{VNDN} \longleftarrow check - trust()$) then
                if ($check(M_{IDsg}, V_{info})M_{IDsg}$)
                $B_{newi}V_{current\,Trust}$
                update TL ⟵$V_{current\,T} + V_{previous\,T}$
                m= True Message ++
                n= False Message ++
           $V_{current\,trust} + + \longleftarrow V_{m+n/m\,trust}$
                update TL ⟵$V_{current\,T} + V_{previous\,T}$
        7. add-new()⟵$B_{newi}$
        8. End
```

Algorithm 2: Policy for the message verification of minor nodes and proof-of-work (Pow) consensus.

```
Steps:
        1. Start
        2. RSU ⟵ send-Msg(VPK)
        3. VNDN ⟵ send(RSU, sessionID)
        4. RSU ⟵ send-signedID(VNDN, sessionID)
        5. SessionID ⟵ check(VPK, Vthreshold)
        6.
if ($time < threshold$) then
                LOC ⟵ publish-LOC (LOC, time, VPK, RSUpK)
            else
               !published()
        7. End
```

Algorithm 3: Proof of location certification issued by RSU.

abnormal requests. By this way, the unnecessary filling of cache can be prohibited. To meet the challenges of unnecessary filling of cache, the detection and defense cache pollution based on clustering (DDCPC) is proposed for NDN. The DDCPC uses three algorithms to calculate the total number of requests, compute the Euclidean distance between all data points, and detect CPAs. The simulation results prove that this is better caching approach in ICN to avoid filling storage and CPAs. In order to track the target, i.e., suspicious vehicle, the authors in [28] proposed a strategy based on pertinence zone having a maximum probability of the presence of the target. The proposed mechanism is divided into two phases, namely, the discovery phase—involving tracking request broadcast, informing entering vehicles about the target, etc., and the tracking phase—involving the detection of target and forwarding reply packets to RSUs. Moreover, for continuous monitoring tracking target, the authors proposed the concept of virtual RSU in the region where real RSU is missing. Virtual RSU is selected on the basis of partitioning of the infrastructure-less region into different clustering zones. Each intermediate vehicle cooperates in tracking a target by broadcasting a message containing detailed information about the target. The vehicle closer to the target acts as virtual RSU for forwarding reply packets to the real RSU. The network architecture is divided into different zones having starting and arrival points. For initiating a tracking process, the central server is a node that acts as an intermediate point between the participating vehicles and an authoritative entity. The proposed strategy has shown an effective way to solve security issues, but the response time is decreased because of checking the content in different tracking zones.

In [29], the authors have proposed a strategy, named blockchain-based anonymous reputation system (BARS), which describes its function, i.e., blockchain, certificate transparency, and components while making assumptions. During system initialization, each vehicle submits its private information including a public key and other legal identification information to law enforcement authority (LEA), which passes the signed warrant to the certificate authority

```
Steps:
    1. Start
2.
if ($T_v < 0.5$) then && ($PRR < threshold$)&&($V < threshold$))    cluster-member($VNDN$)
3.
if ($TRUE$) then
cluster-member() ⟵ Cn
$V_{PID}$ ⟵ allocate(($V_{pk}$, $V_{prk}$))
else
!cluster-member() ⟵ Cn
$M_{NTrust}$ + +                    //Malicious node
4.
if $CH_j > V_{PID}$) then
CH⟵trustable()
CHj++
broadcast(RSU, BS)
RSU⟵save-info()
6. broadcast()
7. End
```

Algorithm 4: Trust evaluation for cluster head (CH) selection.

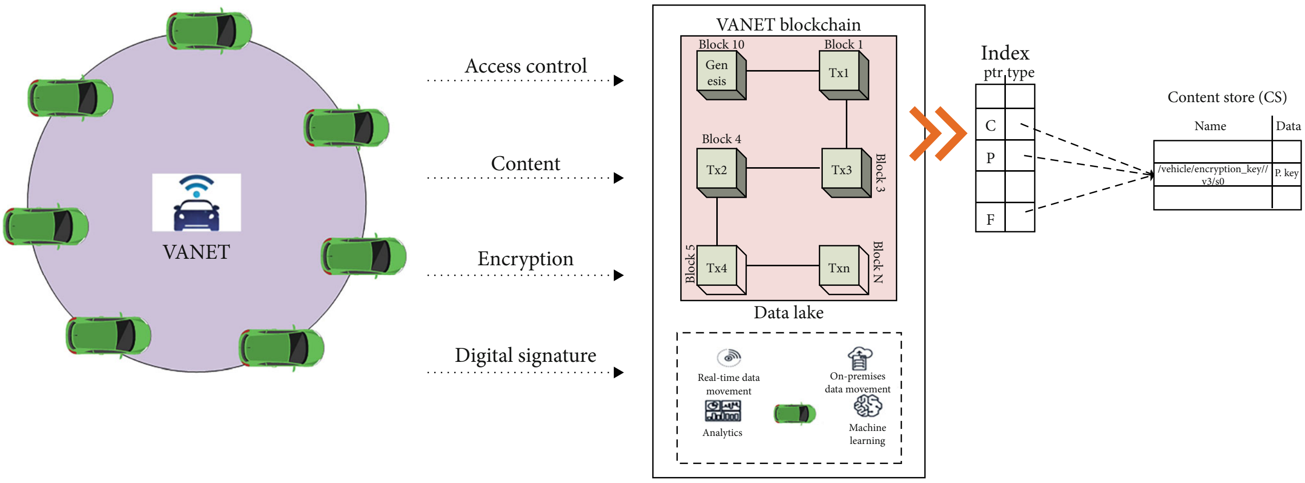

Figure 3: CS for vehicular identification and VANET information retrieval.

(CA) and the CA issues an initial certificate to the vehicle. On the other hand, the LEA receives certificate updating requests from vehicles in one of the three cases, i.e., certificate expiry, threat to private key, or replacement of public key. Next, the updated public key is inserted into revocation blockchain (RevBC) after the verification of RSU based on information broadcast by the CA and LEA during public key revocation. However, the authentication process is used for checking certificate expiry and finding proof of present or proof of absence of a vehicle by matching the root hash value and blockchain for certificate (CerBC) records. This technique provides content security with the expense of content retrieval delay.

```
Steps:
    1. Start
2. CH⟵Algorithm 4
3. $V_{CacheFinal}$ ⟵ $V_{NewTrust}$
4.
if ($V_{contentFinal} \geq CH_{CS}$) then
eviction-policy()
else
accommodate()
5. End
```

Algorithm 5: Cache content on cluster head (CH).

3. Proposed Methodology

In this section, different elements of the proposed mechanism for providing security to content based on blockchain is discussed. The proposed technique provides the mechanism for secure V2V communications through blockchain equipped vehicles in VANETs. We define the K-Mean

```
Steps:
        1. Interest(CH⟵Cn)
2. $C_n$⟵$CH_{Data}$
3.
if ($P_{SignPK} = CH_{PKData}$) then
Cn⟵consume()
else
discard()
new-interest()
4. Stop
```

Algorithm 6: Placement of on-demand data for cluster members (C_n).

cluster head-based minor node selection with push-based and on-demand content placement strategies in the VNDN environment [30]. The SVC-caching strategy provides complete V2V communications in the NDN environment. The proposed approach focuses on the detection of malicious node's intranode trust evaluation policy.

Initially, the vehicle needs to join VNDN by sending vehicle identification (Vid), vehicle public key (Vpk), vehicle private key (Vprk), electronic licence (EL), and trust level (TL).

All the upcoming nodes provide the significance of data and content placement for the vehicle identification authority (BS). Inside the VNDN environment, the vehicles continuously change their positions and the RSU is responsible for tracking the vehicles' location. Due to this, all the above information is stored through RSUs.

The RSU sends data to the BS, which generates the mapping log assigns the Pseudo ID (Pid) and the public and private keys to the Vid. The mapping between the real identity of the vehicle and the Vid was stored in the BS cache [31] for future references in case of a dispute. The TL of the vehicle is set to 0.5. Figure 2 shows the joining of new vehicle and validation process through RSUs. An RSU acts as a validator and provides the validation after the request issued by the vehicle with SID, Kvpl, Locv, CurT, and InitT. The architecture of the proposed strategy is described as follows:

(i) A distributed blockchain trust model is used to add the trustable blockchain in VNDN

(ii) The public key cryptography is used in to provide security for both data and trust evaluation mechanism through blockchain. The emergency messages are kept unencrypted, whereas the infotainment-related messages are encrypted [32]

(iii) At the initial joining, the vehicle normal and minor node selection policy is implemented through a consensus technique, as presented in Algorithms 1, IV-A, and IV-A

(iv) The RSU receives the required VID

(v) The RSU initially checks the joined vehicle's prestored values through vehicle identification VID, vehicle public key and private Key (Vpk, Vprk), EL, CID, and TL

(vi) The BS checks the vehicle identification through a distributed network of VNDN environment and provides a secure message delivery through blockchain

(vii) The RSU also works as a message validator for vehicular nodes (see Algorithm 4.1)

(viii) The RSU issues a proof of location certificate after initial consensus from the vehicular identification and vehicular nodes message validations

(ix) Figure 3 defines the CS Cardenas, an NDN-based secure validation scheme for on-demand content storage (see Algorithm 4-3)

(x) On-demand/infotainment message data requirements inside VNDN are added inside the blockchain on minor nodes and vehicle public and private keys (Vpk, Vprk), which are shared among the VNDN trusted node on-demand

(xi) The Vprk is kept private, and Vpk is shared among all other trustable nodes

(xii) After the final selection of the nodes to become part of VNDN, the content placement is identified [Algorithm 6]

Furthermore, different components involved in the proposed mechanism are discussed in the following subsections.

3.1. Base Station. The BS is a fixed entity in the VNDN environment that maintains the RSUs of a certain area and provides the vehicles' required content. It is responsible for the provision of the keys. Besides, it records the mapping between the real ID and Pseudo ID of the vehicle [33].

3.2. Road Side Unit. The RSU is responsible for the provision of on-demand data from the BS. The legitimate RSU provides the genesis block based on local emergency messages and provides proof of the vehicle's location certificate. It also maintains the log of cluster information. All RSUs (i.e., RSU_{pk} and RSU_{prk}) have a pair of keys that performs validation [34].

3.3. Vehicle. The vehicle has two types in the proposed model, i.e., full node and normal node. The full node has

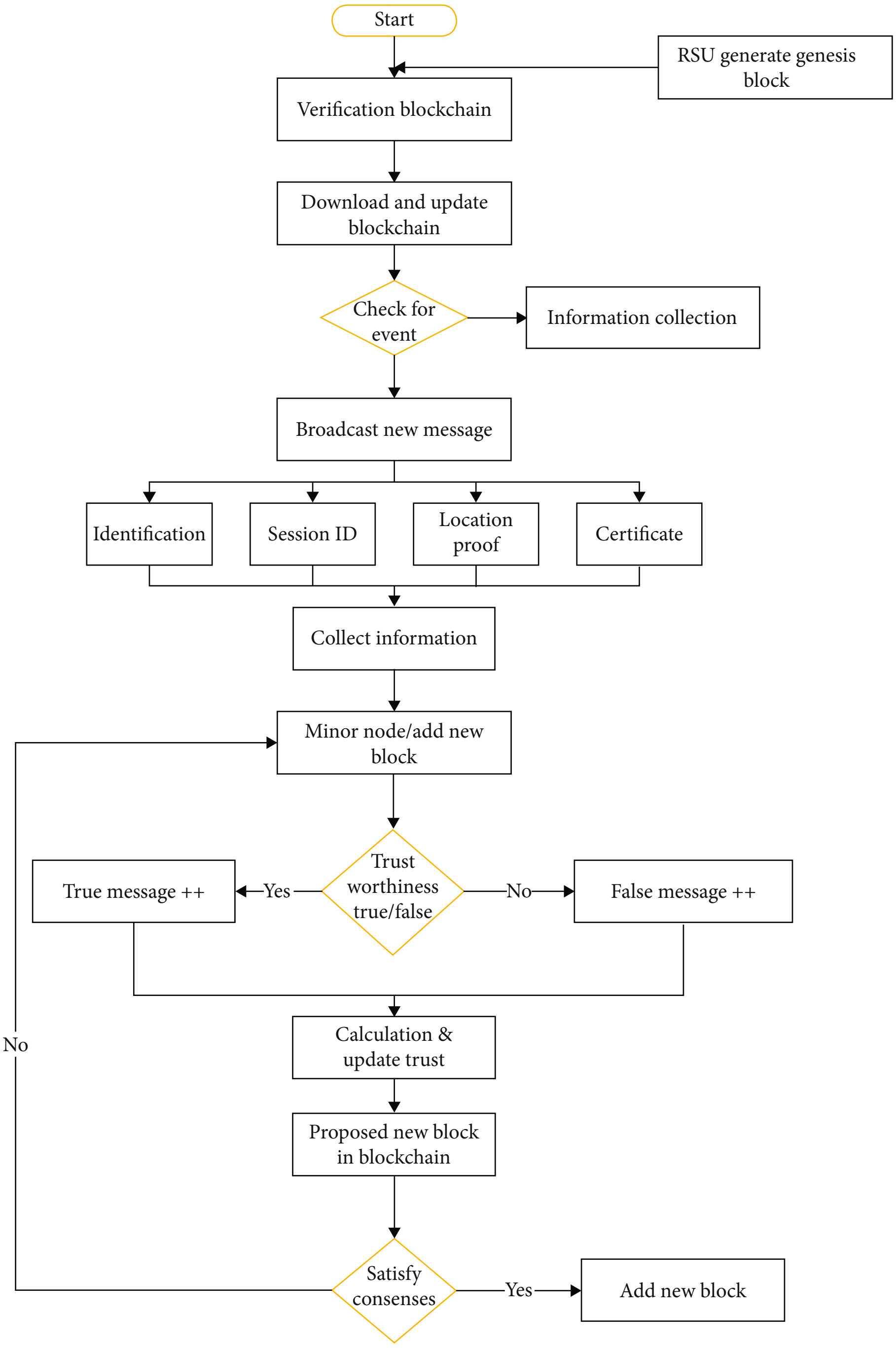

Figure 4: SVC-caching working mechanism.

more computing power and trust than the normal node and mines the new block in the blockchain network. At the same time, the normal node helps in the verification and creation of the event [35].

3.4. Vehicular Named Data Network. In VNDN, there are two types of messages, i.e., emergency/push-based messages and infotainment/on-demand messages.

Since the severity of emergency messages is more, we calculate the vehicle's trust based on emergency messages. The infotainment messages are placed encrypted through a digital signature mechanism of NDN, which is provided on demand of the vehicle.

3.5. Block. Block consists of a block header, which contains information of the previous block hash, timestamp, difficulty target, Merkel root, and a Block body that consists of the event messages as a digital transaction stored on blockchain, added in the main blockchain through the consensus process.

3.6. Proof of Location Certificate. The proof of location certificate is assigned to the vehicle by the respective RSU at a

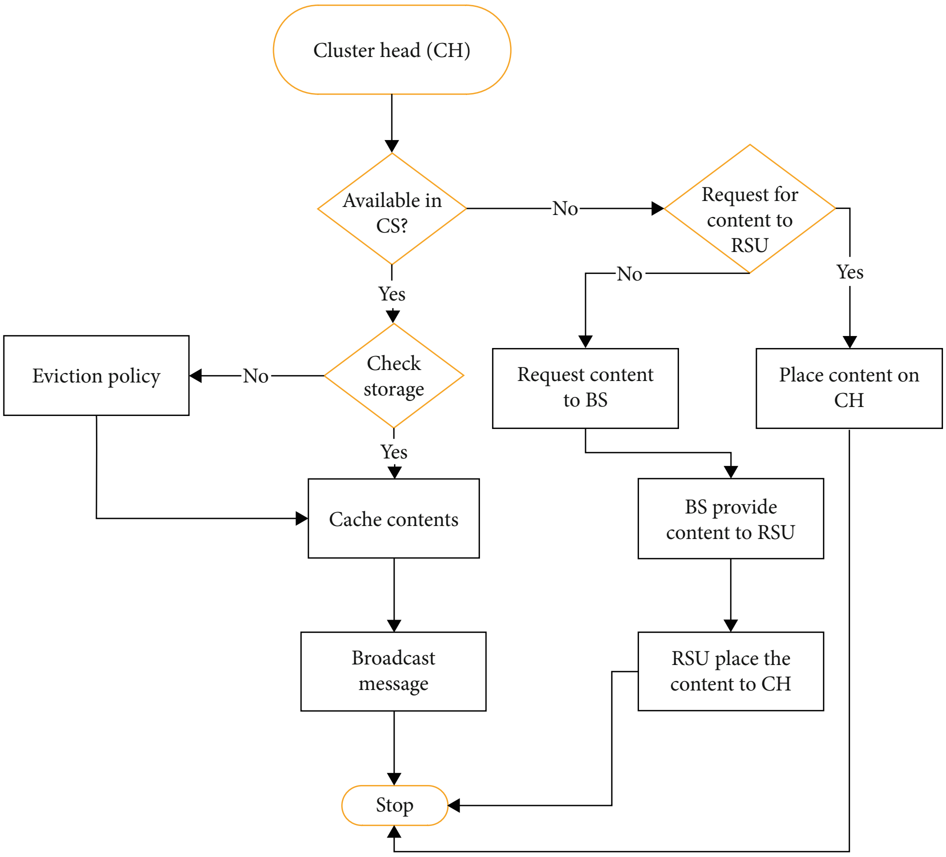

Figure 5: Cache content placement for VNDN SVC-caching.

given time. The RSU acts as a data validator for the vehicle's proof of presence in a particular event.

4. Steps in the Proposed Scheme

All RSUs, i.e., $\mathrm{RSU}_{\mathrm{pk}}$ and $\mathrm{RSU}_{\mathrm{prk}}$, and vehicles have their public and private key pairs (Vpk, Vprk). The vehicle sends a message signed by its public key (Vpk). In reply, the RSU sends a random session ID (SID). The vehicle sends the signed session ID back to RSU [sign(SID)]. The RSU validates the message through (Vpk).

4.1. Threshold Time. The threshold time of response (few milliseconds) is set by the RSU to validate the message. The RSU publishes a LOC to the vehicle including location, time, and public-key (Vpk) signed by the RSU private key ($\mathrm{RSU}_{\mathrm{prk}}$). The POL is used instead of GPS so that the message cannot be spoofed. This alone cannot guarantee the message trustworthiness; therefore, the blockchain mechanism is used.

4.2. SVC-Caching. SVC-caching works the same as that of the NDN caching environment with a security feature embedded to secure minor vehicles' secure content placement. In this approach, we work with two main vehicles, where one is normal node (after verification from RSU through trust threshold values of greater than 0.5 issued by the RSU validation policy) and minor node (for the content placement, which is aimed at controlling the whole verification policy for the efficient management of these nodes with a high level of vehicular trust development). Normal and minor node data are stored in either RSU or BS for the vehicles' future verification. Figure 4 demonstrates the workflow of SVC-caching technique.

Initially, the RSU generates the genesis block to add inside the blockchain. The genesis block is the first block of the blockchain network to secure the blockchain technique. The RSU verifies the blockchain, and then every VNDN verifies, downloads, and updates the existing blockchain. After the initial verification of the blockchain, the VNDN checks for any new event that happens, e.g., a *Request* for the content or content placement in the VNDN environment. The information is collected from the VNDN environment, which is part of the network automation.

The time to select the new node for the normal and minor nodes according to the POL, there is a technique to collect the information. A message is broadcast to all the vehicular nodes to become normal or minor ones. Besides, the threshold values are set to verify the vehicles to add or remove from the blockchain network. The information collected from the vehicles includes MsgID, Session ID, and POL. After the initial validation, the RSU/validator validates and provides the certificate. The whole process continues until it provides the information. After the collection of certification verification, the minor node is selected and added inside the blockchain.

Table 1: Different symbols used in algorithms.

S. No	Legend	Description
1	$V^{\text{Previous}}{}_{\text{T}}$	Previous trust value of the vehicle
2	RSU_{POL}	Check for RSU's proof of location (POL) certificate
3	$V^{\text{RSU}}{}_{\text{Sess ID}}$	Session ID assigned by RSU to vehicle
4	$T^{V}{}_{\text{respond}}$	Response time of the vehicle assigned by RSU
5	$B^{\text{New}}{}_{\text{i}}$	New blockchain
6	H#	Hash of all under event messages
7	$B_{\text{i-1}}$	Hash of the previous blockchain
8	$D_t \longleftarrow \text{coefficient} * 2^{(}8 * ((\text{exp}^{-}3)))$	Target difficulty
9	M_{VNDN}	Messages in the VNDN environment
10	V_{LOC}	Vehicle location
11	$M^{\text{ID}}{}_{\text{sg}}$	Instructions/second (job/task execution speed)
12	$V^{\text{current}}{}_{\text{T}}$	Current trust of the vehicle
13	R	RAM required on memory (in bytes)
14	V_{info}	Vehicle information
15	V	Vehicle velocity threshold: average speed: 30 km/h, urban trunk road: 60 km/h, urban secondary roads: 40 km/h
16	V_{CID}	Vehicular cluster identification
17	$V^{\text{Cache}}{}_{\text{S}}$	Storage of the vehicular caching
18	CH	Cluster head
19	V_d	Vehicle direction
20	$V_{\text{(Clusters)n}}$	Vehicular clusters
21	BS	Base station
22	Threshold	Range (0.1–1.0)
23	trustable-Node	≥0.5
24	malicious-Node	≤5
25	$M^{(\text{N})}{}_{\text{v}}$	Malicious node
26	$V^{(\text{New})}{}_{\text{Trust}}$	Trustable nodes
27	V_{NODE}	Vehicular node
28	CH_{DATA}	Data on the cluster head
29	$P^{\text{Sign}}{}_{\text{PK}}$	Matches the signature of the public key
30	PRR	Previous request rate threshold: 10 interest/sec
31	CH^{j}	Number of times selected as cluster head

4.3. Trustworthiness. The trustworthiness is checked and is shared with all vehicles after the complete validation process, as described in Algorithm 4-1. The values are updated if the trust is true as True Message++ and updated if the trustworthiness is false and calculated as false verification as False message++. The values are updated and the trust computations are calculated according to the suggested values. The new blockchain is proposed in the whole new process. In the next step, a consensus is checked according to the blockchain values. All the consensus is satisfied and provides considerable details to conduct the analysis; i.e., at least 15 vehicles should verify the event message. If it is satisfied, a new block is added inside the blockchain network. If not satisfied, the new minor node is selected for the blockchain validation process.

The process in Figure 5 is used to place the content for the normal and on-demand secure content placement. Till now, we have selected the normal and minor nodes as trustable nodes for the VNDN environment (see Algorithm 4-1). The trustable minor node is selected as the CH, which provides the mechanism to support a temporary adjustment of these nodes because their trustworthiness is calculated, which finally provides the content placement mechanism (see Algorithm 4-3). The CS is used to store on-demand and normal content to provide the content to requested vehicles. After initial requests, if the content is available in the CS, then, the CH storage is checked. The eviction policy [36] is applied in case of insufficient storage; otherwise, the content is placed.

During the checking of the content at the NDN's CS, if the content is not found, then, the request is made for the RSU to store the content. If the content is not found on the RSU's CS, then, content placement does happen. Otherwise, the content request is made through the BS, and the BS provides the content to the RSU to place over the CH for content delivery in VNDN, as presented in Algorithm 4-3. After successful placement of the content, a broadcast message is sent, which contains the public key of the node selected as CH to gather the selected vehicles' content, as demonstrated by Algorithm 6. Based on the policies of the selection of trustable normal nodes, minor nodes, proof of location certification, trust evaluation, and content placement, separate algorithms are proposed for every task to be accomplished in the SVC-caching technique. This technique provides the mechanism for data security through trust and content placement on these trustable vehicles. Table 1 defines all special symbols used inside the content placement technique and provides a complete mechanism to control all these operations. We have provided the security of both on-demand and push-based data in the VNDN environment for secure V2V communications through privacy and trust, which are the main requirements of VANET security.

5. Results and Discussion

The simulations have been performed in the NS-2 simulator to measure the performance of SVC-caching and other strategies, i.e., PNCE, IR, Reactive, and PeRCeIVE. The input parameters for simulations are presented in Table 2. The SVC-caching is a very effective approach to achieve the security and cache placement in the VNDN environment. In addition, it is suitable for the applications of VANET caching schemes. This section elaborates the simulation environment and simulated parameters, which are cache hit, content delivery, one hop ratio, and malicious node detection.

The number of tests is performed to obtain reasonable results. The performance of SVC-caching shows major contributions to the VNDN environment.

5.1. Cache Hit Ratio. The cache hit ratio is set as one parameter explaining the number of cache content found inside the minor nodes' memory. To find the cache hit ratio, the formula presented in Equation (1) is used.

$$\text{Cache hit ratio} = \frac{\text{Total}_{\text{cache}}}{\text{Cache}_{\text{hit}} + \text{Cache}_{\text{miss}}}. \tag{1}$$

Figures 6 and 7 show the cache hit ratios of the proposed scheme in comparison with PNCE and IR techniques with the cache size of 50 and 100 MB. The performance of all techniques increases with the increase of cache size, where the SVC-caching has 15% higher cache hit as compared to PNCE and 60% higher than IR. When the node size reaches 100, the performance of SVC-caching is still stable, as shown in Figure 7. Shortly, SVC-caching has 13% higher cache hit ratio than PNCE and 55% than IR.

5.2. Delivery Ratio. The delivery ratio is linked with the round-trip time. The round-trip time is the total time from data request submission to data received. To calculate the delivery ratio, Equation (2) is used.

Table 2: Simulation environment parameters.

S. No	Parameter	Value
1.	Simulation time	1000 s
2.	Simulation area size	Region 1 Region 2 250 ∗ 250 m 500 ∗ 500 m
3.	Number of vehicles	50 in Region 1 100 in Region 2
4.	Vehicle time for a drive	150 s
5.	Wireless area (single RSU)	200 m
6.	Cache values	0 s to 200 s
7.	Road condition	New entry (one-way road)
8.	RSUs	10
9.	RSU broadcast time interval	50 s
10.	Breakdown duration for vehicles	120 s
11.	Number of simulation runs	200

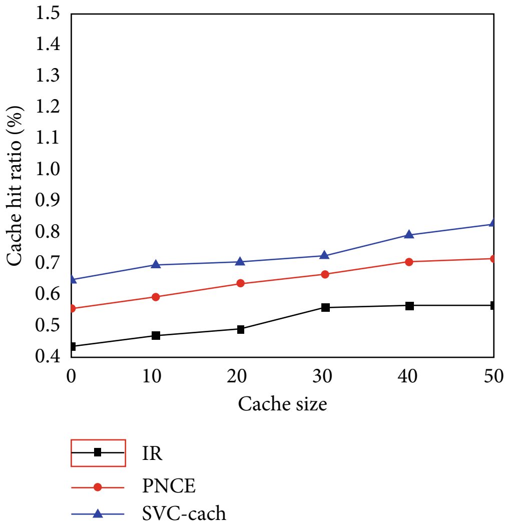

Figure 6: Cache hit ratio for cache size 50 MB.

$$\text{Delivery ratio} = \frac{\text{Packet}_{\text{Receive}}}{\text{Packet}_{\text{sent}}}. \tag{2}$$

Figures 8 and 9 show the delivery ratios under different conditions. It is clear that when the node size increases, the delivery ratio for all techniques increases.

The SVC-caching strategy guarantees higher increase in the delivery ratio with the node size increase because SVC-caching has greater neighbour cache information for vehicles due to CHs. The cache size growth at the IR and PNCE is not increased, whereas in the SVC-caching, the efficiency of the algorithm increases with the increase of cache size.

5.3. One Hop Ratio. The hop count is an essential parameter in the VNDN environment. The hop count illustrates that how many intermediate nodes are involved in the content

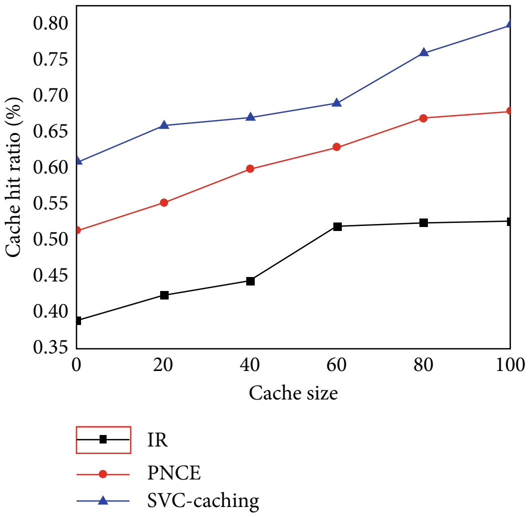

Figure 7: Cache hit ratio for cache size 100 MB.

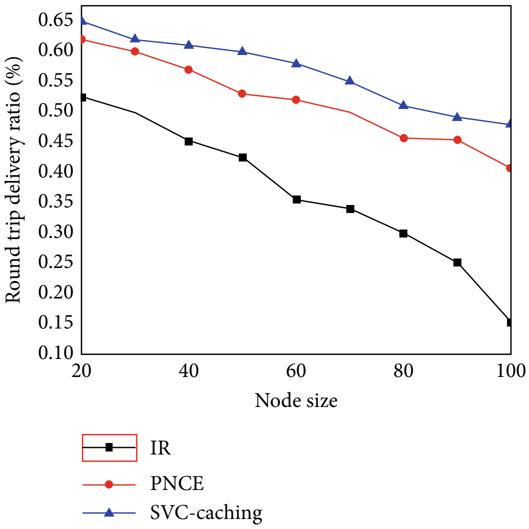

Figure 9: Delivery ratio for node size 100 MB.

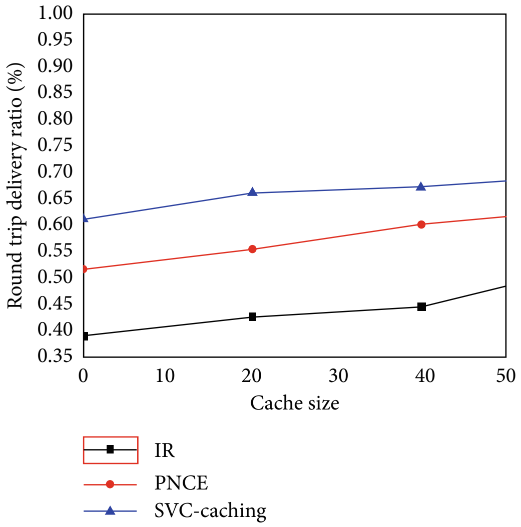

Figure 8: Delivery ratio for node size 50 MB.

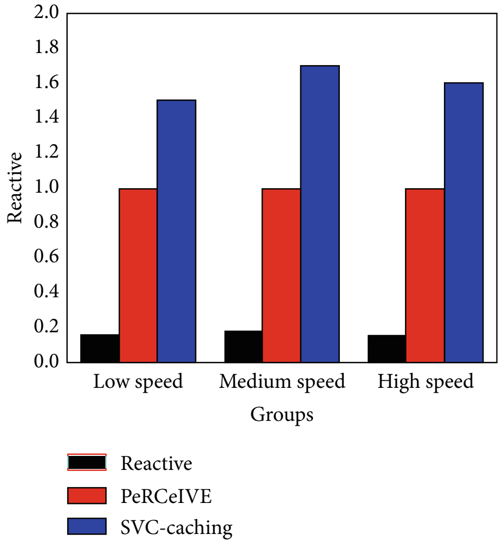

Figure 10: One hop ratio.

request response of vehicles. There is a limited number of nodes linked to provide the necessary details for controlling these parameters. The hope count is calculated through

$$\text{One hop count} = \frac{\text{Request}_{\text{sent}}}{\text{Request}_{\text{respons}} + \text{Responses}_{\text{all}}}. \quad (3)$$

One hop ratio is the comparison of requests sent by vehicles and response between the first hop and all hop responses. The SVC-caching strategy is compared with the PeRCeIVE and reactive caching strategies for the one hop count. To place the cache data on particular selected vehicles based on RSU selection criteria, SVC-caching places higher data rates than other caching techniques based on three vehicle speed parameters, i.e., low speed vehicles, medium speed vehicles, and high speed vehicles. Figure 10 shows the comparison results on the basis of multiple data caching techniques.

At low speed, Reactive shows 0.16, while PeRCeIVE and SVC-caching exhibit 1 and 1.5 ratios, respectively. At medium speed, Reactive, PeRCeIVE, and SVC-caching demonstrate 0.18, 1, and 1.7 ratios, respectively, whereas, at higher speed, the ratios of Reactive, PeRCeIVE, and SVC-caching are 0.15, 1, and 1.5, respectively. At the end, an average of 60% improvement in the one hop ratio of SVC-caching strategy is achieved.

5.4. Malicious Node Detection. Throughout simulations, two regions were selected, i.e., Region 1 and Region 2. Region 1 contains a total of 50 vehicles and Region 2 consists of 100 vehicles. A blockchain-based message validation technique is applied to detect malicious nodes. Malicious nodes are the ones that do not satisfy the criteria to become a member of the cluster. Figure 11 shows a total of 50 vehicles out of which 5 do not pass the RSU's validation criteria to become members of the cluster. Again, the simulations are run in a

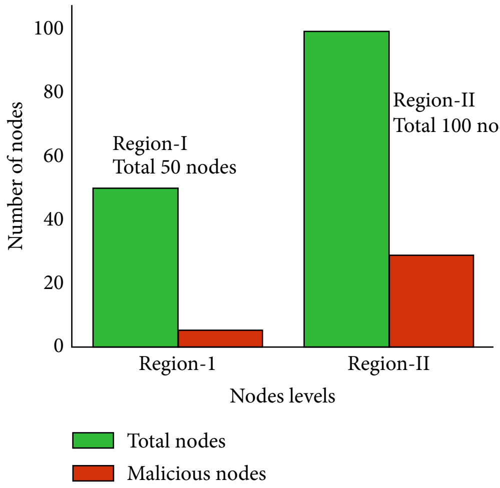

Figure 11: Region 1 and Region 2 malicious node detection.

larger environment, like 100 vehicles, passing through trust management criteria. Out of 100, only 29 vehicles are detected as malicious nodes.

6. Conclusion

A new model for cache placement is proposed, which is well suited for the VNDN environment. Using the blockchain-based distributive trust model is achieved for the eviction of malicious nodes to provide security and reliability of the data. The trust management strategy is adopted for gaining security while placing content on selected nodes. Furthermore, the NDN environment is used for V2V communications, which has multiple advantages over traditional IP-based communications. VANET provides a very effective way for passengers, drivers, and vehicles to exchange content with proper security. The proposed SVC-caching shows superior performance over other caching placement techniques. The results are evaluated based on the following parameters: one-hop count, delivery ratio, cache hit ratio, and malicious node detection. In addition, the proposed mechanism provides an effective way for vehicular communications. Moreover, this technique improves the performance on the basis of selected parameters. In the future, the proposed work can be extended to cloud/fog computing-based VANET environment wherein the communication has a wider range over the simple VANET environment.

Data Availability

This paper is based on simulations, which does not need any dataset.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Cyber Security; in part by FCT/MCTES through national funds and when applicable cofunded EU funds under the project UIDB/50008/2020; and in part by Brazilian National Council for Scientific and Technological Development (CNPq) via Grant No. 313036/2020-9.

References

[1] C. Chen, C. Wang, T. Qiu, M. Atiquzzaman, and D. O. Wu, "Caching in vehicular named data networking: architecture, schemes and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2378–2407, 2020.

[2] G. Ma, Z. Chen, J. Cao, Z. Guo, Y. Jiang, and X. Guo, "A tentative comparison on cdn and ndn," in *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2893–2898, San Diego, CA, USA, October 2014.

[3] I. U. Din, S. Hassan, A. Almogren, F. Ayub, and M. Guizani, "PUC: Packet Update Caching for energy efficient IoT-based information-centric networking," *Future Generation Computer Systems*, vol. 111, pp. 634–643, 2020.

[4] S. Hassan, I. U. Din, A. Habbal, and N. H. Zakaria, "A popularity based caching strategy for the future internet," in *2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT)*, pp. 1–8, Bangkok, Thailand, November 2016.

[5] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies - CoNEXT '09*, pp. 1–12, Rome, Italy, December 2009.

[6] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of VANET clustering techniques," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 657–681, 2016.

[7] J. M. Duarte, T. Braun, and L. A. Villas, "Source mobility in vehicular named-data networking: an overview," in *Ad Hoc Networks*, pp. 83–93, Springer, 2018.

[8] X. Wang and H. Qian, "Constructing a 6lowpan wireless sensor network based on a cluster tree," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 3, pp. 1398–1405, 2012.

[9] J. Y. Kim and H. K. Choi, "An enhanced security protocol for VANET-based entertainment services," *IEICE Transactions on Communications*, vol. E95.B, no. 7, pp. 2245–2256, 2012.

[10] O. A. Khan, M. A. Shah, I. Ud Din et al., "Leveraging named data networking for fragmented networks in smart metropolitan cities," *IEEE Access*, vol. 6, pp. 75899–75911, 2018.

[11] S. Ul Islam, H. A. Khattak, J. M. Pierson et al., "Leveraging utilization as performance metric for CDN enabled energy efficient internet of things," *Measurement*, vol. 147, article 106814, 2019.

[12] D. Grewe, M. Wagner, and H. Frey, "PeRCeIVE: proactive caching in ICN-based VANETs," in *2016 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, Columbus, OH, USA, December 2016.

[13] M. Duan, C. Zhang, Y. Li, W. Xu, X. Ji, and B. Liu, "Neighbor cache explore routing protocol for VANET based on trajectory prediction," in *2018 IEEE 3rd Advanced Information*

Technology, Electronic and Automation Control Conference (IAEAC), pp. 771–776, Chongqing, China, October 2018.

[14] W. Xu, X. Ji, C. Zhang, and B. Liu, "Nihr: name/id hybrid routing in information-centric VANET," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Seoul, Korea (South), May 2020.

[15] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "A security solution for v2v communication within VANETs," in *2018 Wireless Days (WD)*, pp. 181–183, Dubai, United Arab Emirates, April 2018.

[16] H. Sun, S. Y. Lee, K. Joo, H. Jin, and D. H. Lee, "Catch id if you can: dynamic id virtualization mechanism for the controller area network," *IEEE Access*, vol. 7, pp. 158237–158249, 2019.

[17] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, "Reputation-based blockchain for secure ndn caching in vehicular networks," in *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–6, Paris, France, October 2018.

[18] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 464–467, PyeongChang, Korea (South), February 2017.

[19] H. A. Khattak, K. Tehreem, A. Almogren, Z. Ameer, I. U. Din, and M. Adnan, "Dynamic pricing in industrial internet of things: blockchain application for energy management in smart cities," *Journal of Information Security and Applications*, vol. 55, article 102615, 2020.

[20] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "Ftm-iomt: fuzzy-based trust management for preventing Sybil attacks in internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4485–4497, 2020.

[21] M. A. Judge, A. Manzoor, H. A. Khattak, I. Ud Din, A. Almogren, and M. Adnan, "Secure transmission lines monitoring and efficient electricity management in ultra-reliable low latency industrial Internet of Things," *Computer Standards & Interfaces*, vol. 77, article 103500, 2021.

[22] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc: a security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[23] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2020.

[24] I. U. Din, A. Bano, K. A. Awan, A. Almogren, A. Altameem, and M. Guizani, "LightTrust: lightweight trust management for edge devices in industrial internet of things," *IEEE Internet of Things Journal*, 2021.

[25] W. Huang, T. Song, Y. Yang, and Y. Zhang, "Cluster-based cooperative caching with mobility prediction in vehicular named data networking," *IEEE Access*, vol. 7, pp. 23442–23458, 2019.

[26] M. Chowdhury, A. Gawande, and L. Wang, "Secure information sharing among autonomous vehicles in ndn," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pp. 15–25, New York, NY, USA, April 2017.

[27] L. Yao, Z. Fan, J. Deng, X. Fan, and G. Wu, "Detection and defense of cache pollution attacks using clustering in named data networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, 2020.

[28] A. Derder, S. Moussaoui, Z. Doukha, and A. Boualouache, "An online target tracking protocol for vehicular ad hoc networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 969–988, 2019.

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

[30] I. Hussain and C. Bingcai, "Cluster formation and cluster head selection approach for vehicle ad-hoc network (VANETs) using k-means and Floyd-Warshall technique," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, p. 01, 2017.

[31] L. Cárdenas-Robledo and A. Peña-Ayala, "Ubiquitous learning: a systematic review," *Telematics and Informatics*, vol. 35, no. 5, pp. 1097–1132, 2018.

[32] D. S. P. K. Nirmala, "Probabilistic mceliece public-key cryptography based identity authentication for secured communication in VANET," *Solid State Technology*, vol. 63, no. 6, 2020.

[33] A. R. Abdellah, A. Muthanna, and A. Koucheryavy, "Robust estimation of VANET performance-based robust neural networks learning," *Learning*, vol. 11660, pp. 402–414, 2019.

[34] R. Zhang, F. Yan, W. Xia, S. Xing, Y. Wu, and L. Shen, "An optimal roadside unit placement method for VANET localization," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–6, Singapore, December 2017.

[35] M. H. Alwan, K. N. Ramli, Y. A. al-Jawher, A. Z. Sameen, and H. F. Mahdi, "Performance comparison between 802.11 and 802.11p for high speed vehicle in VANET," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3687–3694, 2019.

[36] Y.-T. Yu and M. Gerla, "Information-centric VANETs: a study of content routing design alternatives," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, Kauai, HI, USA, February 2016.