Manchester Metropolitan University

e-space

Manchester Metropolitan University's Research Repository

Please cite the Published Version

Ali, A, Iqbal, MM, Jabbar, S, Asghar, MN, Raza, U and Al-Turjman, F (2022) VABLOCK: a blockchain-based secure communication in V2V network using ICN network support technology. Microprocessors and Microsystems, 93. p. 104569. ISSN 0141-9331

DOI: https://doi.org/10.1016/j.micpro.2022.104569

Publisher: Elsevier

Version: Accepted Version

Downloaded from: https://e-space.mmu.ac.uk/630125/

Usage rights: Creative Commons: Attribution-Noncommercial-No Derivative Works 4.0

Additional Information: This is an Accepted Manuscript of an article which appeared in Microprocessors and Microsystems, published by Elsevier

Enquiries:
If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines)

Journal Pre-proof

VABLOCK: A BLOCKCHAIN-BASED SECURE COMMUNICATION IN V2V NETWORK USING ICN NETWORK SUPPORT TECHNOLOGY

Abid Ali , Muhammad Munwar Iqbalb , Sohail Jabbar , Muhammad Nabeel Asghar , Umar Raza , Fadi Al-Turjman

PII: S0141-9331(22)00121-1
DOI: https://doi.org/10.1016/j.micpro.2022.104569
Reference: MICPRO 104569

To appear in: *Microprocessors and Microsystems*

Received date: 15 January 2021
Revised date: 28 December 2021
Accepted date: 18 February 2022

Please cite this article as: Abid Ali , Muhammad Munwar Iqbalb , Sohail Jabbar , Muhammad Nabeel Asghar , Umar Raza , Fadi Al-Turjman , VABLOCK: A BLOCKCHAIN-BASED SECURE COMMUNICATION IN V2V NETWORK USING ICN NETWORK SUPPORT TECHNOLOGY, *Microprocessors and Microsystems* (2022), doi: https://doi.org/10.1016/j.micpro.2022.104569

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2022 Published by Elsevier B.V.

Journal Pre-proof

VABLOCK: A BLOCKCHAIN-BASED SECURE COMMUNICATION IN V2V NETWORK USING ICN NETWORK SUPPORT TECHNOLOGY

[1]Abid Ali, [1]Muhammad Munwar Iqbal, [2]Sohail Jabbar, [3]Muhammad Nabeel Asghar, [4]Umar Raza, [5]Fadi Al-Turjman

[1]Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan
[2]Department of Computational Sciences, The University of Faisalabad, Faisalabad, Pakistan
[3]Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan
[4]Department of Engineering, Manchester Metropolitan University, United Kingdom
[5]Artificial Intelligence Dept., Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

abidali.hzr@gmail.com, munwariq@gmail.com, sohail.jabbar@tuf.edu.pk, nabeel.asghar@bzu.edu.pk, u.raza@mmu.ac.uk, fadi.alturjman@neu.edu.tr

Abstract

Vehicular Ad hoc Network (VANET) provides efficient communication among vehicles (V2V). The communication among all the vehicles complies with the on-demand, which contains a secure and trustable mechanism to ensure trustable communication. The modification in the communication information may result in falsified information. Secure data is very important in V2V communication to save the lives of pedestrians and drives by delivering secure and accurate information. To address the problem and achieve secure communication in V2V, we proposed a new blockchain-based message dissemination technique to secure V2V communication. With the passive need for adaptable and sufficient content delivery, information-centric networking (ICN) is adopted to enhance trustworthiness communication in VANET. We used Cluster-based secure communication through ICN-based VANETs. As VANET is open, ICN provides direct content requests and responses without location dependency. ICN-based VANET enhances caching abilities. The blockchain-based security protocol is implemented to secure efficient communication without altering the messages. The protocol achieves privacy, security, and trust for detecting malicious nodes in VANET. Additionally, the Clustering technique is applied to adopt in-range communication. Proposed-Caching framework enhances security and provides on-demand data to vehicles. NS-2 simulator is used to simulate the Proposed VABLOCK approach. Experimental results are performed and compared with relevant techniques, which show enhanced results based on cache hit ratio, one hop count, malicious node detection, and delivery ratio. We demonstrate that proposed caching improves results on selected parameters based on results.

Journal Pre-proof

Keywords: *Vehicular Adhoc Network (VANET), Information-Centric Networking (ICN), Blockchain, Vehicle-to-Vehicle (V2V) Communication, Base Station, Data Security, Internet Of Things (IoT).*

I. Introduction

Nowadays, vehicles communication is necessary to connect IoT Devices, Vehicles, Road Side Units (RSUs). Communication and transmission are necessary to connect all the vehicles towards effective data transmission. Communication among vehicles leads towards new communication technology called Vehicular Adhoc Network (VANET). In VANET, the vehicles communicate and provide communication among their Road Side Units (RSU). VANET consisted of Onboard chips/Units (OBU) and Road Side Units (RSU). In VANET, vehicles move objects, and RSUs are installed on Road Sides [1].

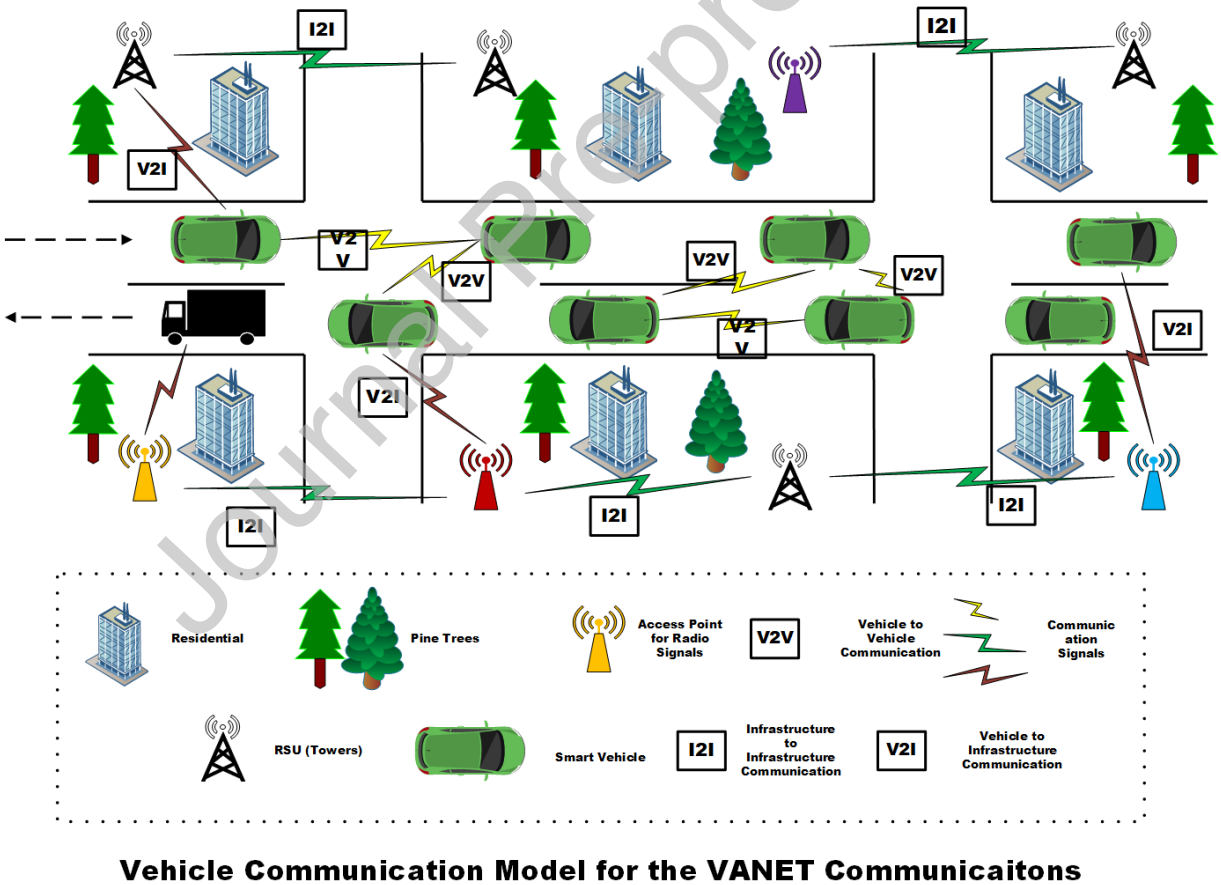

Figure 1: Complete Vehicular Communication with RSU, BS, Vehicles, Access Points over I2I, I2V, and V2V model.[2]

Journal Pre-proof

Journal Pre-proof

VANET communication is possible through three main categories. One is Vehicle to Vehicle (V2V), the second is Vehicle to Infrastructure (V2I), and the third is Infrastructure to Infrastructure (I2I). V2V is possible among vehicles only through wireless communication. In V2I, communication is possible through fixed RSUs, and in I2I is through fixed infrastructure [3]. RSUs are installed on the road sides of the highway and motorways, so these provide a communication backbone. Figure 1 describes the Infrastructure of VANET.

One server is installed to control the whole communication possible through VANET, i.e., Base Station (BS) or Manager, which control the whole VANET infrastructure and communication. BS and RSU control everything that lies for infrastructure-based communication. These handle whole protocols and other measurements for infrastructure and other communication ways. In this paper, we consider V2V communication among vehicle nodes. Our basic concept is to provide communication among the vehicle under a secure communication channel. VANET communication enhances the safety of the roads, reduce much amount of traffic congestion handling, vehicles information sharing, road conditions, traffic control information sharing, sharing of the contents among the vehicles, sharing road safety information among vehicles, conditions of the current traffic under the control information among the vehicles that are relevant for the information-based. VANET can provide information, internet content, and multimedia content information in addition to all this information. For a few decades, Vehicular Ad-Hoc Networking (VANET) has gained popularity in industries and research academia for its intelligence and secure transportations system. Effective traffic monitoring system and management of current traffic conditions VANET is best appropriate to deploy is the traditional vehicular transportation system [4]. Traditional IP-based communication for vehicles makes VANET more prone to malicious attacks.

VANET provides constraints for communication among Vehicles to support and maintain the Quality of Service (QoS). All services and applications inside VANET are handled after maintaining QoS [5]. Inside VANET, two types of nodes exist. One type provides a control message, and the second provides content delivery. Request and response to share contents are handled through Information-Centric Networking (ICN). ICN shifts content requests from the host to content-centric. Content sharing is possible through name-based communication rather IP based. In this paper, we focused only on ICN-based communication in VANET. Name Data Network

(NDN) is only name-based which supports ICN architecture for communication. Infrastructure-based communication is only possible when ICN involve, and IP-based is discouraged in all communication channels of ICN based communication. ICN-based NDN communication is more secure than IP-based communication. ICN is consisted of Pending Interest Table (PIT), Forwarding Information Base (FIB), and Content Store (CS) [6-8]. Figure 2 explains VANET architecture.

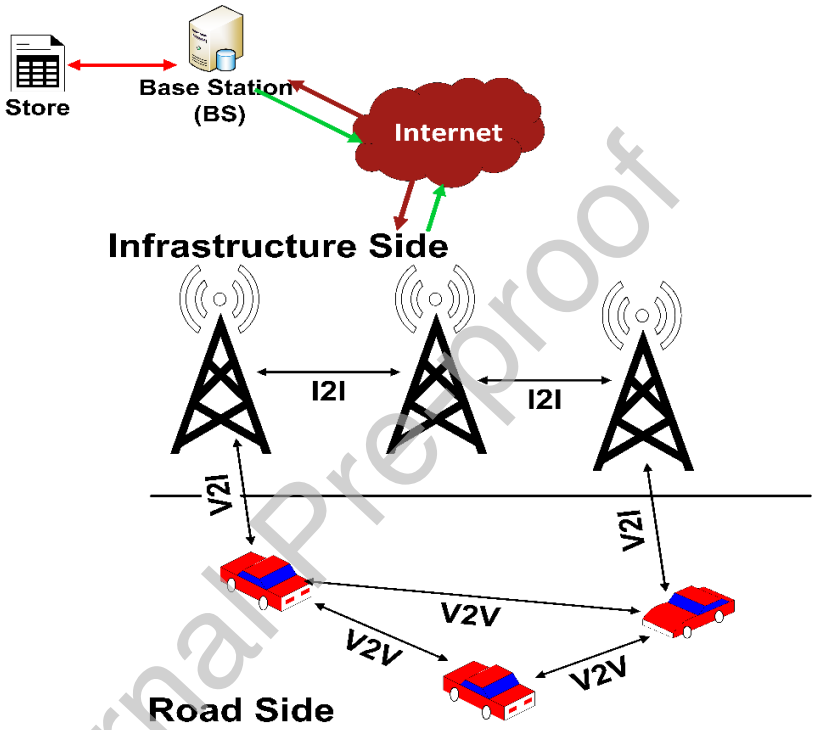

Figure2: VANET Infrastructure [9]

Journal Pre-proof

This paper focused on ICN-based VANET to share content, control signals, and other relevant information among vehicles. Through clustering, vehicles are selected to store content. These handle all requests coming from other request vehicles—CS in NDN cache the content from RSU on Cluster Head (CH) from every cluster. The content is retrieved from BS to RSU to CH in every cluster. All content interfaces and vehicle records are stored on PIT for incoming requests.

Moreover, PIT also creates backlink baths from hope to hope and puts an entry into the PIT requests table. Finally, FIB searches for prefix and matches the relevant content to arrange the

Journal Pre-proof

prefix-based communication in VANET [10]. Figure 2 depicts the ICN-based data transmission in VANET.

Although, ICN provides effective connectivity among vehicles to control and provide reliable communication to choose clusters and Cluster Heads (CH) selection. We consider security and trust management issues for CH selection as VANET is an ever-changing environment which makes CH a challenging task. We consider that the cluster-based selection of CH is a critical task in VANET. In this paper, compromised requests originating from malicious nodes are handled specifically using V2V communication. After malicious information, the authenticity of VANET is compromised, and messages are broadcast through V2V communication. This causes accidents, traffic incidents, and some serious issues to distribute among all vehicles in VNDN based VANET. To improve the VANET, many researchers improve VANET security based on multiple environments, password encryption methodology, RSU based security implementation. Based on the discussion, we are not sure that we can handle on-demand security issues in the VANET environment [11].

Therefore, this research article proposed a Vehicles cluster-based blockchain trustable security mechanism that effectively detects the malicious nodes and their attacks in V2V communication in a highly dynamic environment. We introduced the Proposed-Caching strategy to cache the content using NDN with blockchain-based trust-based security establishment in VANET. We have considered that Proposed-Caching provides secure NDN content placement on vehicles after selecting the CH, such as traffic information and popular data. Still, this information placement is very difficult in high dynamic nature. Proposed-Caching technique in V2V communication selects CH as Cache Node and cache content for normal nodes to use cached content. Proposed-Caching reveals a malicious request. In VANETs, the vehicle should have the capability to communicate and exchange information continuously.

Secure communication between vehicles without considering the vehicle's physical location, there is a need for a communication mechanism to achieve secure communication between vehicles. A mechanism is proposed which will help provide the above-said advantages. Security is the main risk in VANETs due to the user's data availability. Thus, there should be some secure and trusted mechanism for VANETs to provide trust during communications. The main purpose of the VANET is to provide safety to passengers and share route information such as traffic conditions

Journal Pre-proof

and weather. This mechanism will provide secure on-demand communication between vehicles in two different domains. The ICN architecture is used in which data security is not a problem since the naming is used for data. The proposed mechanism will authenticate the sender as well as the receiver. This mechanism also detects the non-trusted vehicle based on communication experiences. The main contributions of this paper are listed below:

1. We propose the Proposed-Caching strategy that uses blockchain-based trustable V2V communication among the high dynamic vehicles.
2. The selection of Cluster Nodes (CNs) and CH uses a customized K-Means dynamic clustering algorithm.
3. We have presented the Proposed-Caching strategy to place the content using the SND approach for inter-vehicle communication that organizes the communication in vehicles in the same mobility patterns as all vehicles can perform.
4. Proposed-Caching enhances reliable content caching and requests handling in VANET using V2V communication.

The paper's organization is as follows: Section II reviews related research for VANET V2V communication and security aspects. Section III presented the proposed-caching strategy to enhance the V2V secure communication using cluster-based information communication in the NDN environment. In section IV, we presented the results and discussion section to enhance the results presented in this research article. Discussion and Evaluation are also discussed in this section of the research article. All contributions and presentations are discussed and presented in section V. In section VI of the research, we present the conclusion and some future recommendations.

Journal Pre-proof

II. Related Work:

In VANET, various methodologies are proposed to secure and share the content in the VANET environment. Pros and cons are associated with each methodology. In this section, we discuss existing caching methodologies proposed in the VANET environment.

The Authors in [12] proposed the Lave Copy Everywhere (LCE) method, which cache content on all nodes that lie in the publisher and subscriber's path. It cached the content once, and the copy is available for all future requests. Redundancy is increased, and more space is consumed. In [13]

PNCE method is proposed. Is worked on name-based content addressing. It reduces the packet delay and finds optimal paths for packets dissemination. It also improves round trip time but increases the packet forwarding complication and network congestion in VANET. Authors in [14] proposed member and leader-based grouping to secure V2V communication. Asymmetric key encryption and distribution are adopted in all nodes. Multi-hop communication infrastructure is proposed to secure and cache the content. Trust computation is performed to increase the network performance and detect malicious nodes. Still, delay in the content placement and retrieval is identified over the network performance and network enhancement.

The data request and response idea in VANET is introduced by [12], which is traditionally IP-based LTE-V communication. This approach introduced the pre-fetching of the data context for the VANET environment. Cooperative and non-cooperative caching are introduced with the high availability of the nodes for effective communication. In non-cooperative, all nodes share non-caching information [13], whereas cooperative nodes share cached information to reduce the redundancy in caching and delay access[14-17]. Group-based V2V communication is introduced in [20], using a Group-based leader and other communication members. Systematic keys are used to establish links among the group's leaders and members. In [18], A neighbor cache explore routing protocol is introduced. An in-centric caching strategy is introduced to effectively reduce the redundant packets from the network and choose the path optimal for transmitting forwarding information in the VANET environment. In [19], the COMP approach is introduced. The proposed algorithm groups the similar patterns vehicles in a single cluster with the help of prediction techniques for effective cache improvement and network performance. In [22], the authors introduced a new approach based on a trustable vehicle identification approach for vehicle protection and authenticate the information before fulfilling the vehicle's request for the content. In Perceive [20], the authors proposed new chunks based on the hierarchical namespace to place the content.

Moreover, chunks of two types are one for requested data calculations, and the other for data distributions. The authors [24] proposed a new approach to detecting attacks generated by malicious nodes in the VANET environment. The basic aim is to detect the Cache Pollution attacks (CPAs). This approach uses clustering to detect CPA and applies a defensive DDCPC approach against the detections. Furthermore, the Authors in [21] proposed the discovery and tracking

mechanism. The first algorithm tracks the request broadcasted for the target and other target detection and sends feedback to RSU. Authors in [26] introduced a cluster-based cooperative caching strategy. Clusters are transforming with inter-cluster and intra-cluster communication to enhance the mobility of the proposed technique. The proposed technique enhances the caching and VANET performance for effective collaboration with the proposed approach. Cooperative caching strategy stops false dissemination of messages from V2V network and protects nodes tracking through pseudonym approach. The delay in the content retrieval is also improved with the proposed technique. Besides all these, a cooperative caching technique enhance retrieval time, and content placement hop counts.

III-System Architecture of VANET Secure Communications using Blockchain

Blockchain has revolutionized the VANET security achievement. Decentralized and distributed technology of the Blockchain plays a significant role in maintaining security in the VNDN. More specifically, in the V2V communication, there is no direct involvement of the RSU to establish and maintain security. The scenario of Secure VNDN communication based on blockchain technology is illustrated in figure 3. The graphical representation VNDN blockchain manages and updates the complete Vehicle registration, data collection, and Cache data placement on the Vehicles.

The Cache vehicles' data stores act as a separate repository for content placement such as Map Routes, Road Coordinates, Weather conditions, etc. Stored-Off blockchain network formed using data storage and delivery. It encrypts data with the digital signature. Data Lake that presents the cache contents based on the most trustable vehicles is a useful tool for tasks such as Visualizations, Analytics, and Reports presentations. Figure 3 shows Blockchain and ICN-based VANET model to predict effective and reliable content delivery. It helps the VANET community and the Disaster Management Departments, Government Departments, and other related departments store extensive data. This blockchain-based network can share the content among the vehicles, RSU's, and other related centralized BSs. All these data access permissions are allowed using the access control policy in the smart trust management contract adopted by the VNEND blockchain network to preserve the content store's integrity and privacy.

Journal Pre-proof

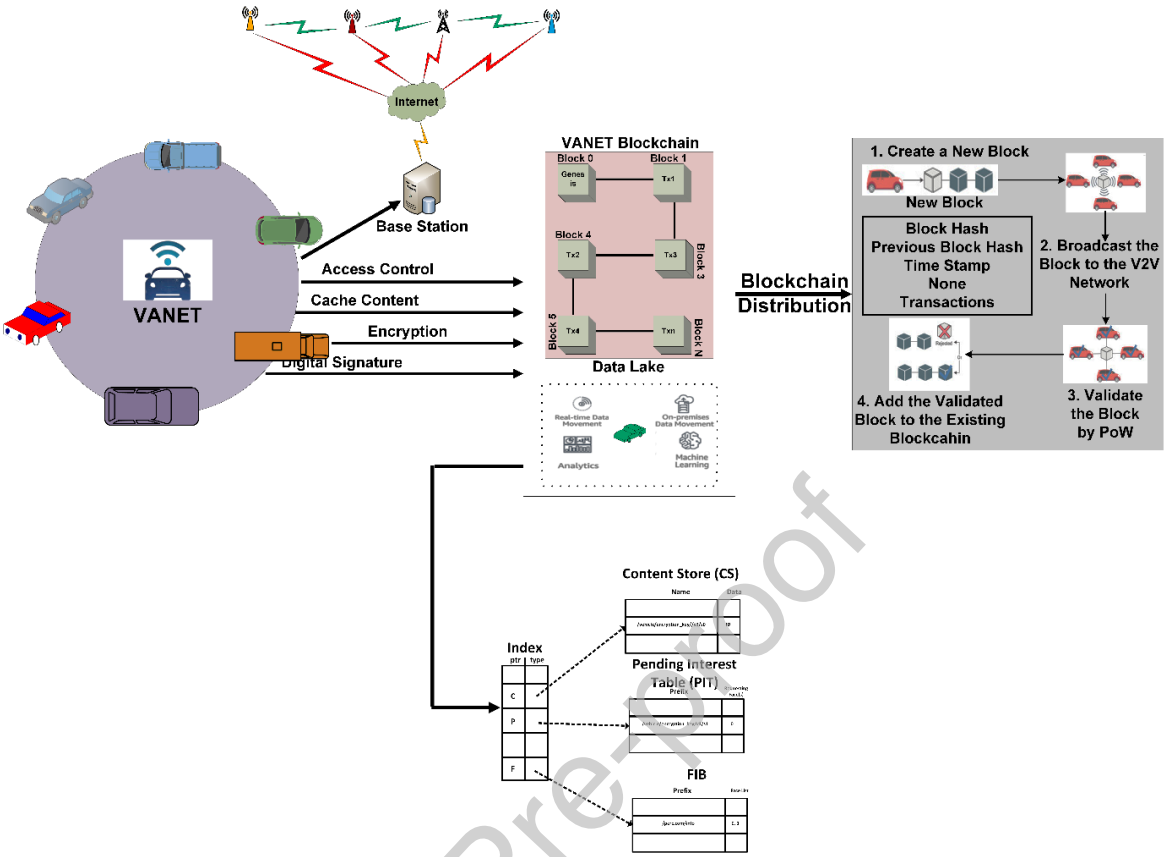

Figure3: Scenario of VANET based ICN communication in a VANET blockchain

In the proposed technique, we considered two main nodes, i.e., VN and Road Side Unit (RS U) nodes. RSU and VN store data structures like FIB, PIT, and CS in the ICN-based NDN environment. The V_{id}, $V_{content}$, and Trust computation V_{tr} is saved inside the Blockchain to distribute the effective formulation blockchain network. The VN_{id} is stored inside the CS of ICN communication to link the ICN with the Blockchain.

The Blockchain is responsible for storing the trust values, VN history, and event messages in an encrypted format. Every encounter vehicle broadcasts the messages to other vehicles inside the events. The Blockchain validates the incoming vehicular nodes' trusts and saves the trust values using V_{id} to validate the trust computations. The proposed technique is shown in figure 4. It consists of main features: 1) K-mean clustering for cluster transformation, 2) Trust Computation using decentralized blockchain technology, 3) The Caching algorithm that placed the content on the trustable Vehicles using Blockchain storing encryption and digital technology. ICN is used to consult for the network computation among the VNs and then share the content based on the ICN

Journal Pre-proof

methodology. This research aims to develop the trust computations model using decentralized blockchain technology to secure cache placement on trusted VN.

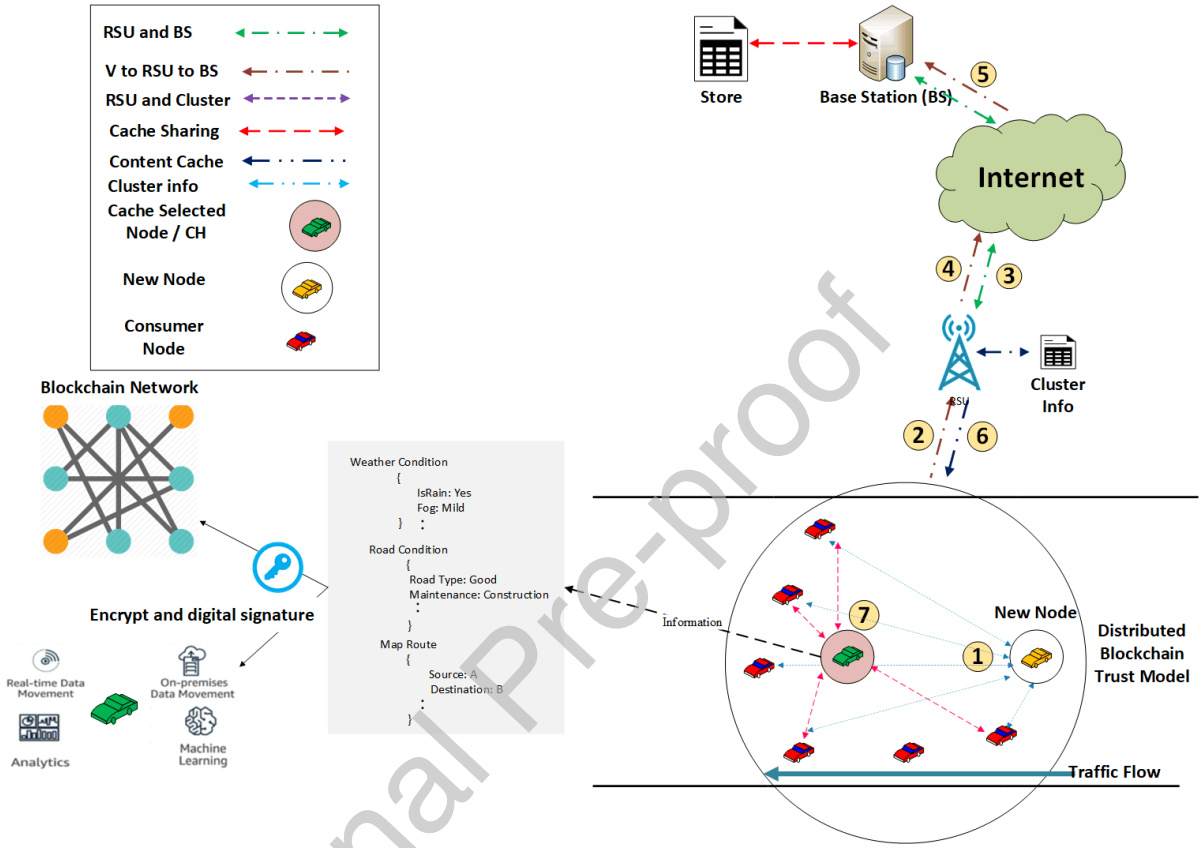

Figure 4: Scenario of Content Caching and Placement in secure VANET environment using Blockchain Technology

Cluster Transformation using K-Means Clustering [6]

Selected CHs are used to place the caching data effectively. BS is the main part of generating and distributing the content to RSU's, and then RSU places the content based on ICN-based selected CHs for every cluster. However, we are working with only the V2V part of the communication in VANET. Hence, RSU's responsibility is only to place the content on select CH from all VNs after calculating their trust computations using the blockchain technique. Blockchain message dissemination security control is applied using multiple packages applied through this approach.

Journal Pre-proof

The CH selection procedure is based on the RSU request-response, i.e., RSU first fetches information like Cluster range, Vehicle direction, Velocity, Number of clusters, Cluster centers, and the number of times selected as CH The illustration of the Proposed-Caching working is described as When a new node is entered into the VANET environment as a new VN RSU fetches the newly entered vehicle identification number with other RSU's present in VANET. The new VN becomes a member of the cluster. BS/RSU verify and assign a new identification number to the new VN. The vehicle contains the old ID, which is already registered. If the ID is not registered, the vehicle will show as unknown of VN. The new request will be discarded from RS U/BS. The database is maintained alongside the BS for entering The VN information. The blockchain distribution mechanism is used to calculate the trust management of the VN that enters the cluster. Blockchain is applied to the peer-reviewed message dissemination from the vehicles. Node's validation is measured using the blockchain message dissemination technique, and results are compared using the trust threshold value to calculate the final trust value. All those nodes that pass the trustfulness criteria are registered in the RSU. A copy of the trusted vehicle in the form of flags is broadcast to the RSU's. Then all RSU's transmit this copy to all registered vehicles in the clusters.

Assume that the content that we place as cooperative caching after nodes selection as cluster head based on the cluster head selection for content placement is expressed in equation 1.

$$C_j \leftarrow \frac{1}{|P_c|} \sum_{p_c \in P_c} N_n * R_C \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Cluster transformation is based on the RSU location, and its domain of signals through which the VN is allowed to transmit and resolve their request and response issues for NDN based data in CS CH is selected using the previous trust values, the number of times previous CH counting, velocity, speed, and actual position in the cluster. VN with the cluster center is preferred as CH compared to other VNs. Moreover, the contents are placed using the VNDN CS placement strategy after being selected as CH. All VNs then request the content copy from the CH nodes of every cluster. Figure 4. demonstrates the process of the proposed methodology for cluster transformation, trust evaluation, and calculations, and lastly, place the cached content on the selected CH.

Event Proof

The vehicle information such as speed, heading, location, and road conditions are exchanged for awareness in the cooperative package, such as the trust computation using the blockchain message

dissemination technique. Based on the VN event change, every vehicle request is sent within the selected cluster after 100 ms time. The receiver data should be valid based on abnormal traffic, road hazard, weather conditions, or other traffic conditions. Information from the VNs is shared based on the $\boldsymbol{VN_{id}}$. In the proposed model of the content placement on trusted nodes in the proposed technique, the VN shares the $\boldsymbol{VN_{id}}$ with the near VN in the corresponding cluster, and the need checks each $\boldsymbol{VN_{id}}$ by VNs. The event is triggered, and near VNs, verify the generated message.

Moreover, the blockchain services are enabled by every VN that lies inside the cluster verification. The complete procedure of the cache placement using V2V Blockchain and ICN-based secure communication is shown in figure 5. Discussion about the flow diagram in figure 5 is discussed in the section below.

The mechanism is a complete VANET secure content placement using blockchain-based communication. Initially, the VN_{id} is shared among all the VNs of the particular Clusters Nodes (CNs). VNid is verified by the RSU after verification as already a part of a network or a new node. RSU check this node from the existing nodes as ID from a set of existing nodes $N_p = \{N_1, N_2, N_3, \ldots. N_m\}$. If the new node is not part of the set of existing nodes, the node is infected or declared as malicious as all registered nodes are confirmed part of that node. The threshold values to be selected using the vehicle registration algorithm VR (VN_{id}, P_t, C_t).

On the other hand, VN joined the Blockchain using its ID As for as, and the VN is already part of the event EN, that node joined Blockchain. A message broadcast technique is applied to disseminate the peer VNs. Moreover, message validation is performed with peer nodes to justify the messages as trustable nodes. The trust values TVN are calculated, and values match for TVN with the threshold Tr using CH inside the existing threshold values.

Journal Pre-proof

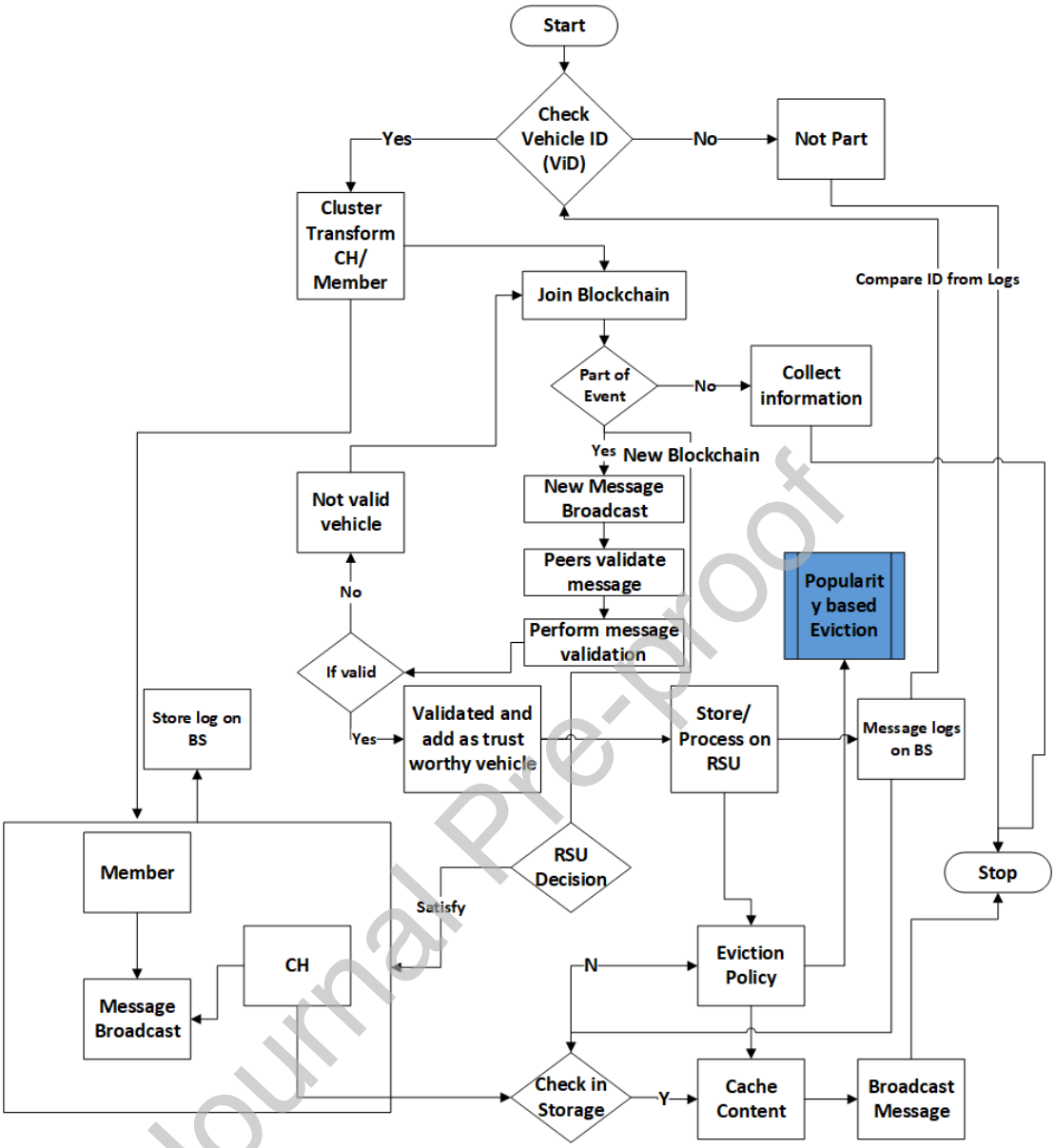

Figure5: Flow of Proposed secure content placement in VANET

BB

Moreover, the validation performed is stored inside the Blockchain with Vid, and a copy of the V_{id} is also stored inside the ICN, CS, for communication purposes. The Tv validity relies on trust threshold value where $T_v \geq 1$, VN of respective VN_{id} will declare as valid, and its content is stored in the Blockchain, and V_{id} is stored in CS, and when $Tv \leq 1$, the vehicle is not declared as valid. The blockchain trust computation again is computed and verified. For future correspondence, a copy of the content is also placed on RSU to BS. Through the eviction policy, the highest trustable

Journal Pre-proof

node is selected for the content placement through equation 2. The message counters count the messages as true or false from VPNs. If the messages are trued, then saved for the trust computations; otherwise, messages were discarded where m and n are counters.

$$\mathbf{M} \approx \begin{cases} \boldsymbol{if\ true\ then, m++} \\ \boldsymbol{if\ false\ then, n++} \end{cases} \quad \text{..... [7]}$$

The confirmation of the valid Vehicle the $\boldsymbol{T_v}$ is stored in the proposed blockchain network's data structure. The data that is proposed is ideal for getting back the results. The content is placed inside the trusted vehicles. The trustworthy VNs for every cluster are computed using the below section.

Trust Computation Using Blockchain

The trust computation using the blockchain message dissemination technique begins working after storing the previous trust values $\boldsymbol{T_{Tv}}$ inside the VNDN. The trust computation in VNDN was performed on the vehicle side. $\boldsymbol{V_{Tr}}$ has computed the trust value for every ***VN*** in the network. After loading every VN blockchain from the previous phase, the vehicle checks the received ***MsgBC*** for every vehicle inside the cluster. Moreover, based on the previous uploads, the messages option is checked; if the MsgBC is not updated, then the $\boldsymbol{V_{Tr}}$ is considered the same for participation in VNDN. However, if the MsgBC is updated from the previous state, the VNDN calculates a new trust value. We have proposed to secure the events and messages generated using Blockchain. New trust values are calculated for every ***VN*** whose $\boldsymbol{V_{Tr}}$ is updated from the previous updates. Trust Offset is calculated if the MsgBC is updated from the previous updates. Before the latest MsgBC update, if the VN sends an MsgBC, then no need to update the $\boldsymbol{V_{Tr}}$**.**

When the clusters are formed, CH and VN are identified for the trusts' final computation based on the blockchain message dissemination technique. The CH is selected to place the content, but before that from CH, set the transformation of VN to CH is the very trustful job for the Proposed-Caching to select the CH and then calculate the trust for cache placement for RS U. Trust computation is calculated to select the trustable CHs for effective and trustful placement of the cache contents.

To select the CH, we have used to blockchain message dissemination technique. Initially, we declared this blockchain technique as a private blockchain with BS as the central authority to handle all the Blockchain of messages. After addressing the above issues raised for the cache placement, we have proposed the scheme that used the Interest Satisfaction Rate (ISR) and Previous Request Rate (PRR) for the appropriate content to place the cached content on the CHs.

RSU_{req}^{n} Places the results based on the request rates for every V.N. Proposed-Caching placed the cached content on the respected cache node for accessing all trustable VN dynamically.

Trust computation is described in Algorithm 1. The selected CHs only participated in the trust computations because content cache placement is done on these nodes. The blockchain message dissemination scheme is used based on the peer validation process. A member is selected from algorithm 1 as a CH node. RSU first fetches the content from the H as VID, PRR, and v. RSU then validates the current trust information from BS and makes a list of CH with ISR and CHs. However, based on the blockchain message dissemination technique for effective content placement. After selecting CH as trustable nodes, the RSU broadcast messages to all Proposed-Caching members.

Algorithm 1: Trust Algorithm

V_{id} = Vehicle Identity

V_d = Vehicle Direction

$C_n^{(Clusters)}$= Vehicle Direction

B_s = Base Station

V_{trust} = Vehicular Trust

$M_v^{(N)}$= Malicious Node

$V_{Trust}^{(New)}$= Vehicle Direction

Output: Trust Evaluation

Procedure:

1. Start
2. $C_n^{New} \leftarrow \sum_{j=1}^{k}\sum_{i=1}^{n} || \ x_i^j - \ x_j||^2$
3. $M_{new}^{Cache} \leftarrow C_n^{New}$
4. for i ← n

$V_{new}^{Cache} \leftarrow$ f(M_{Node}^{CS})

$if\,(V_{new}^{Cache} \geq event())$

$Q_v^{CH,RSU} \leftarrow$ validation()

Journal Pre-proof

$M_{final}^{CH} \leftarrow \sum_{j=1}^{n} j \; / \; N_1^N$

$if\,(M_{final}^{CH} \geq threahold())$

validate() $\leftarrow M_{Trust}^{N}$

$V_{Trust}^{New} + +$

else

!validate()

$V_{node}^{N} \leftarrow M_V^N$

$V_{Trust}^{New} - -$

else

!validate()

5. End.

Cache Algorithm

According to the cache placement schemes and selection of the CH node for cache placement, RSU placed the cached content on the CH' according to the selected cache placement scheme. This approach did not place the same content on every CH. The interesting content is placed on the CHs because placing the same cache content on the same data source may cause the redundancy and waste of the resources that cause the deprivation in the cache placement scheme's performance. Algorithm 2 define content caching on selected CH node. The algorithm effectively enhances the eviction policy to improve cache placement performance by utilizing the cache resources effectively.

Algorithm 2: Cache Algorithm

v = Vehicle velocity

V_{CID} = Vehicle Cluster ID

V_S^{Cache}= Vehicle Cache Storage

CH = Cluster Head

Output: Cache Content

Procedure:

Journal Pre-proof

1. Start
2. CH ← $Algorithm\ 1$
3. $V_{final}^{Cache} \leftarrow V_{Tust}^{New}$
4. $if(V_{final}^{Cache} \leftarrow V_{previous}^{Cache})$
5. $flag \leftarrow FALSE$
6. discard(eviction_policy())
7. $else\ if(V_{final}^{content} \geq V_S^C)$
8. $flag \leftarrow TRUE$

eviction_policy()

else

accomodate()

B($V_{CID}^{(M)}$)

9. End.

Evaluation

We implemented the Proposed-Caching methodology using Network Simulator-2 (NS-2). We have used PNCE and IR for comparison as a benchmark for this methodology. Due to this, IR and PNCE use the same algorithm for trajectory prediction. In the simulation, we selected two regions: 250m wide and 250m wide, and the other is 500m wide and 500m wide. Vehicles traffic location files are generated from the vehicular maps files discussed in the main model. These files are generated for 250 seconds. To simulate the roads' real conditions, VN is equipped with traffic lights, crossroads, acceleration, Vehicular Identification, traffic lights, and random locations of VNs.Inside all simulations, we have used 802.11b radios at the physical layer, on the link-layer, we have applied Ad-hocMac, and on the Transport layer, we have designed the UDP protocol. For simulation, we have selected the client-server model in NS-2 for simulations. The CH nodes act as the server, and other VNs are served as clients, and clients periodically send the data packets for the request to server nodes for content, and server nodes respond to the Data Packet with content. In the simulation setup, we generated 50 VN's for the first and 100 VN's for the second regions. There are 5 clusters in regions-1 and 10 clusters in region-2, with one CH in every cluster. We have selected 150 types of content, and every provider holds 60 types. The parameters for

Journal Pre-proof

simulation with configuration detail are listed in the table. Table 1 illustrates the whole simulation parameters with their respective values.

Table 1: Configuration Table for simulation parameters

Parameter	Value
Simulation Time	1000s
Simulation area size	Region 1: 250*250m; Region 2: 500*500m
Number of Vehicles	50 in region 1 100 in region 2
Vehicle Time for a drive	150 s
Wireless area (Single R.S. U)	200 m
Cache values	0s to 200s
Road Condition	New Entry (One-way Road)
RSUs	10
RSU broadcast time interval	50 s
Breakdowns duration for vehicles	120 s
Number of simulations run	200
Blockchain policy	Trust Computation

We have introduced three parameters to check the quality of work as matrics

- **Cache Hit Ratio:** Cache Hit Ratio is the total interest packers for content over packets in a normal node cache. Equation 3 defines the cache hit ration formula for Evaluation.

Journal Pre-proof

$$\text{Cache Hit Ratio} = \frac{\sum_{i=1}^{n} C_{hits}}{\sum_{j=1}^{n} C_{hots} + \sum_{k=1}^{n} CS_{mis}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

- **Round Trip Delivery Ratio (RTDR):** The total number of data packets is divided by all numbers of requests for interest packets. Equation 4 defines the Round Trip Delivery Ratio (STDR).

$$RTDR \leftarrow \left(\frac{\sum_{j=1}^{n} \boldsymbol{p_i}}{\sum_{k=1}^{n} \boldsymbol{r_j}}\right) \times 100 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

- **One Hope Ratio:** Request initiated by first hope and received from first hope is the One Hope Ratio.
- **Malicious Nodes Detection:** the comparison of requests Detect the number of affected Vehicles from all 50 vehicles in region-1 and 100 Vehicles from Region-2.

We compared the Proposed-Caching strategy with IR and PNCE approach under node size, Cache size, and malicious node detection parameters through graphs.

1. **Cache Hit Ratio**

In this Evaluation, we compare our proposed technique with IR and PNCE. The proposed technique shows better results than other techniques. Figure 6 and Figure 7 show the Cache Hit Ratio performance. Node size 75 and node size 150 are taken for results comparison when cache ratio in percentage increased then the performance of other techniques. Proposed-Caching show is 60% higher than IR and 15% higher than PNCE techniques. When node sizes go to 150 in figure 7, the proposed system's performance is still increasing. Figure 7 shows 55% of results improvement then IR and 23% then PNCE.

Journal Pre-proof

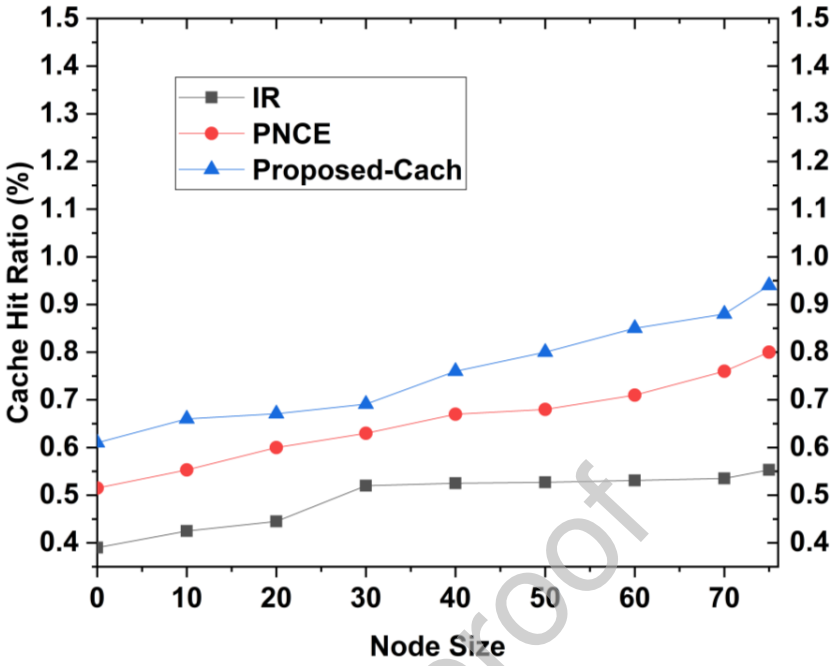

Figure6: Cache Hit Ratio over Node Size 75

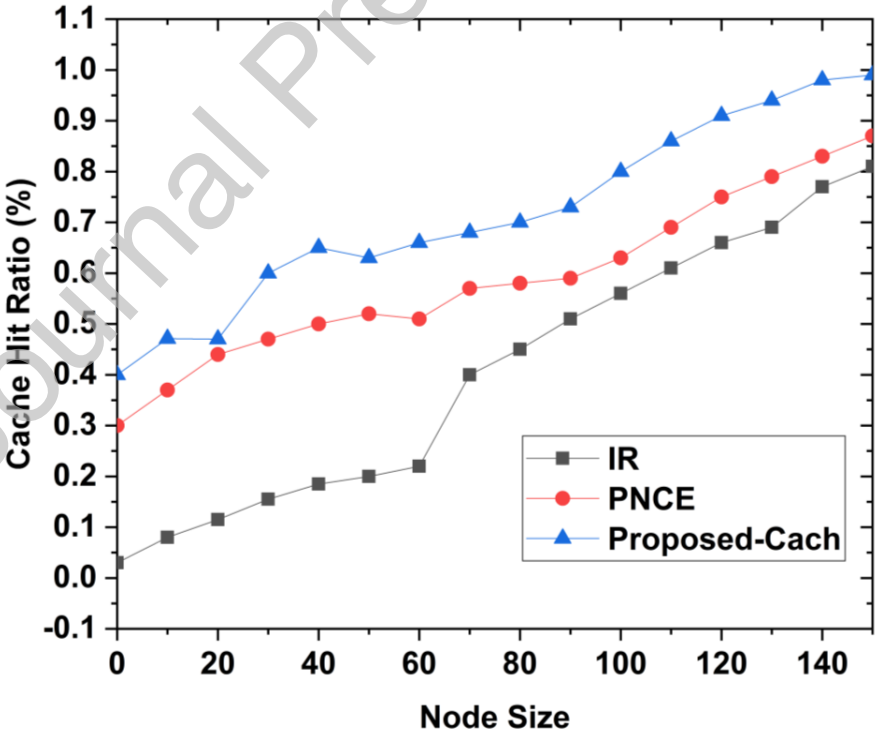

Figure7: Cache Hit Ratio over Node Size 150

Journal Pre-proof

2. Round Trip Delivery Ratio

Round Trip Delivery Ration is expected to increase for complete request submission to completion for cache content. Figures 8 and 9 show cache size with Round Trip Delivery Ration percentage. Figures 8 and 9 show that with the increase of cache size. We compare the delivery ratio with IR and PNCE. Figure 8 shows the delivery ratio for cache size 50. The proposed technique shows that the delivery ratio is also increasing with effective results for the proposed system. 54% higher than IR and 20% higher results than PNCE delivery ratio. The Proposed-Caching strategy shows a higher increase in the delivery ratio with the cache size increase that shows us to the delivery ratio of Proposed-Caching is higher than IR and PNCE because Proposed-Caching has greater neighbor caching information for vehicles in respect of CHs Cache growth size at the IR and PNCE is not increased at the variable-ratio, while in Proposed-Caching, increasing the algorithm's efficiency increases.

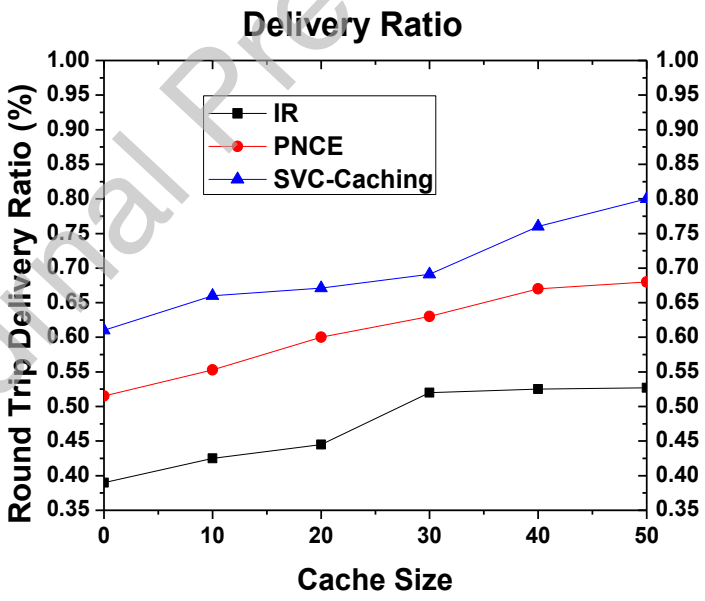

Figure8: Round Trip Delivery Ratio for Cache Size 50

Journal Pre-proof

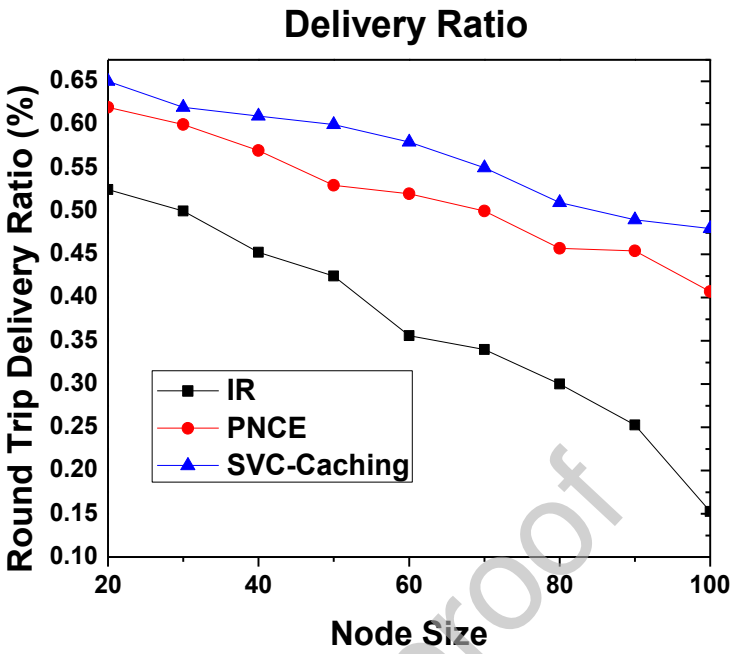

Figure9: Delivery Ratio for Node size 100

3. One Hop Ratio

One Hop count is an evaluation parameter to access the simulation results obtained through the proposed technique. One Hop Ratio is the ratio of the vehicle's request and the first response received by the vehicle. One Hop Ratio results are The Proposed Caching results for One Hop Count are compared with Ractive and PeRCeIVE caching strategies. The caching process is described in section 3 of the paper, where RSU selection criteria and other main requirements are mentioned. The results from figure 10 show that the proposed caching technique develops higher results than other techniques. Three parameters for vehicle speed are considered. Low Speed, Medium Speed, and High-Speed vehicles.

From figure 10, PeRCeIVE shows a 0.18 ratio at low-speed, Reactive shows 0.16 ratio, and proposed caching shows a 1.7 ratio. At the Medium speed of vehicles, Reactive shows the ratios of 0.18, PeRCeIVE shows 1, and Proposed-Caching shows the 1.7 ratios. However, at High-speed vehicles, the Reactive shows 0.15, PeRCeIVE shows 1, and Proposed-Caching shows the 1.5

Journal Pre-proof

ratios. In the end, an average 60% improvement in results of the Hope-Ratio count of the Proposed-Caching strategy.

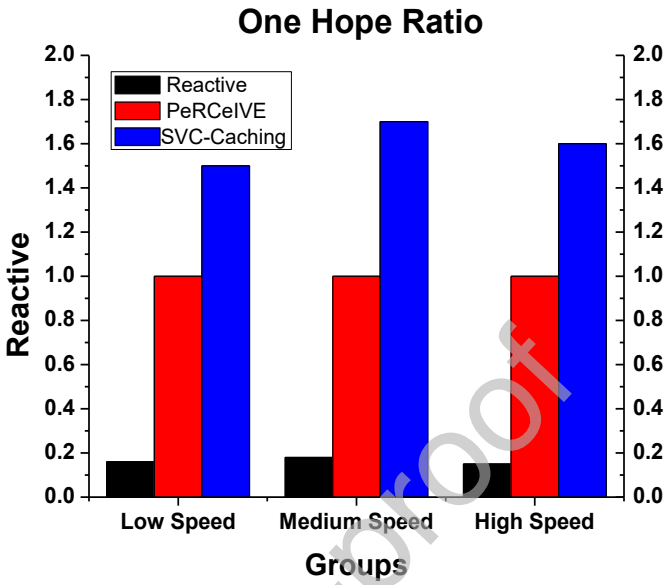

Figure10: One Hop Ratio

4. Malicious Nodes Detection

Two regions for simulations are selected. One is of 40 vehicles and the second is of 100 vehicles. We use Blockchain to detect malicious nodes. Distributed Messages Dissemination Technique is used to detect malicious nodes from the proposed technique. Based on the proposed technique, the malicious nodes are early identified and become part of the cluster after fulfilled criteria. B From figure 11, we show that 50 and 100 vehicles are used for region-1 and region-2. From 50 vehicle regions, there are 5 vehicles identified as malicious nodes. Region-2 contains 100 vehicles. From them, 29 vehicles are identified as malicious using simulation. It represents that our proposed model successfully identifies the malicious nodes in the VANET.

Journal Pre-proof

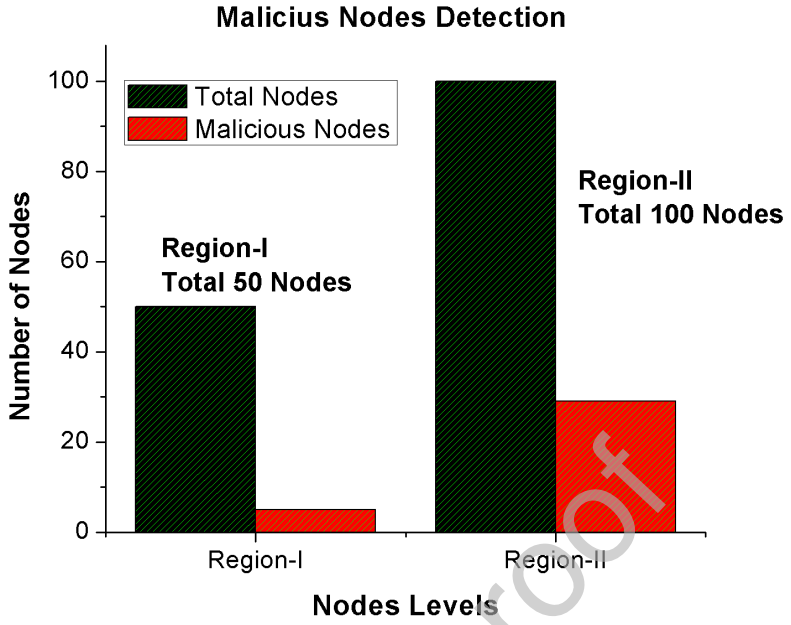

Figure11: malicious Nodes detection in Region-1 and Region-2

Conclusion

This paper proposes a multi-level trust management framework to efficiently manage the dynamic allocation of on-demand cache content in V2V communication. Trust management and secure message communication are still open for VANET communications. We have detected the malicious nodes in our approach and provided an on-demand caching approach in the VANET environment. Trust evaluation is calculation statistically and dynamically. A new model for on-demand cache placement on CH is proposed to enhance network efficiency. Additionally, through trust computation, the proposed system detects malicious nodes and discard request that originated from such nodes. Malicious nodes are evicted, and only trustable nodes are added and participate in V2V communication. The proposed-Caching framework uses a VNDN environment that enhances the efficiency of the network and detects more malicious nodes. Therefore, this research technique prescribes a secure and robust trustable secure V2V communication through secure blockchain architecture. The proposed solution was developed to mitigate VANET network attacks and secure and reliable communication among all the vehicular nodes. The results effectively evaluate the proposed-caching system performance over cache hit ratio, one hop count, malicious node detection, and content delivery ratio. The results are compared with the existing

Journal Pre-proof

technique and declared improved performance over selected techniques. In the future, the proposed mechanism can be implemented through Machine Learning techniques to effectively and in real-time detection of malicious nodes. Moreover, Machine Learning models can predict the proposed system performance early and improve cache placement on CH nodes. CH can also be effectively detected through Machine Learning to improve the system performance.

References

[1] A. K. Goyal, G. Agarwal, and A. K. Tripathi, "Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey," *International Journal of Computer Network & Information Security*, vol. 11, no. 10, 2019.

[2] M. Wang, C. Xu, S. Jia, J. Guan, and L. A. Grieco, "Preference-aware Fast Interest Forwarding for video streaming in information-centric VANETs," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1-7: IEEE.

[3] W. B. Jaballah, M. Conti, and C. Lal, "A survey on software-defined VANETs: benefits, challenges, and future directions," *arXiv preprint arXiv:1904.04577*, 2019.

[4] H. Khelifi *et al.*, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Communications Surveys & Tutorials*, 2019.

[5] M. S. Haghighi and Z. Aziminejad, "Highly Anonymous Mobility-Tolerant Location-based Onion Routing for VANETs," *IEEE Internet of Things Journal*, 2019.

[6] A. Bansal, M. Sharma, and S. J. I. J. o. C. A. Goel, "Improved k-mean clustering algorithm for prediction analysis using classification technique in data mining," vol. 157, no. 6, pp. 0975-8887, 2017.

[7] F. Ye *et al.*, "MISIM: An End-to-End Neural Code Similarity System," 2020.

[8] X. Liu, R. Ravindran, and G.-Q. Wang, "Information centric networking based service centric networking," ed: Google Patents, 2019.

[9] S. Salsano, N. Blefari-Melazzi, A. Detti, G. Morabito, and L. Veltri, "Information centric networking over SDN and OpenFlow: Architectural aspects and experiments on the OFELIA testbed," *Computer Networks*, vol. 57, no. 16, pp. 3207-3221, 2013.

[10] K. Yu *et al.*, "Information-Centric Networking: Research and Standardization Status," *IEEE Access*, vol. 7, pp. 126164-126176, 2019.

[11] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7-20, 2017.

[12] A. Mahmood, C. Casetti, C.-F. Chiasserini, P. Giaccone, and J. Harri, "Mobility-aware edge caching for connected cars," in *2016 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 2016, pp. 1-8: IEEE.

[13] I. Psaras, W. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric," *ICN'12 - ACM Proceedings of the Information-Centric Networking Workshop*, 08/17 2012.

[14] Z. Li and G. Simon, "Time-shifted tv in content centric networks: The case for cooperative in-network caching," in *2011 IEEE international conference on communications (ICC)*, 2011, pp. 1-6: IEEE.

[15] K. Cho, M. Lee, K. Park, T. T. Kwon, Y. Choi, and S. Pack, "WAVE: Popularity-based and collaborative in-network caching for content-oriented networks," in *2012 Proceedings IEEE INFOCOM Workshops*, 2012, pp. 316-321: IEEE.

[16] S. Saha, A. Lukyanenko, and A. Ylä-Jääski, "Cooperative caching through routing control in information-centric networks," in *2013 Proceedings IEEE INFOCOM*, 2013, pp. 100-104: IEEE.

Journal Pre-proof

[17] J. M. Wang, J. Zhang, and B. Bensaou, "Intra-AS cooperative caching for content-centric networks," in *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*, 2013, pp. 61-66.
[18] 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)*, 2018, pp. 771-776: IEEE.
[19] 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.
[20] D. Grewe, M. Wagner, and H. Frey, "PeRCeIVE: Proactive caching in ICN-based VANETs," in *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, pp. 1-8: IEEE.
[21] 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.

Journal Pre-proof

Author's Biography

Mr. Abid Ali is pursuing his Ph.D. degree in Computer Science at the Department of Computer Science, The University of Engineering and Technology Taxila Pakistan. He did his MS(CS) from the same institution in 2018. He is currently serving as a Lecturer in Computer Science in Higher Education Department KPK Pakistan. He has 8 years of teaching and 3 years of research experience. His Currently Research interests are IoT, Distributed Computing, Big Data, Task Scheduling, Data mining, Cloud and Mobile Cloud Computing and ICN.

Dr. MUHAMMAD MUNWAR IQBAL received his M.Sc. degree in Computer Science from the University of the Punjab, Lahore. He received his degree in MS Computer Science from COMSATS Institute of Information Technology, Lahore, in 2011. He completed his degree Doctor of Philosophy in Computer Science from the Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan. He is currently working as Assistant Professor at the Department of Computer Science, University of Engineering and Technology Taxila, Pakistan. He is potential reviewer of HEC NRPU Project, International journals, National journals and conferences. He had published 55 research publications in international journals and conferences. His research area is the Internet of Things, Information-Centric Networking, Machine Learning, Databases, Data Science, Data Mining, Semantic Web, Social Media Analysis, Artificial Intelligence and Machine Learning.

Dr. SOHAIL JABBAR served in different academic and managerial positions at National Textile University, COMSATS University Islamabad, and Bahria University, Islamabad, where he also headed different research groups. He also served as a Postdoctoral Fellow with the CfACS IoT Lab, Manchester Metropolitan University. Currently, he is serving as Associate Professor and Associate Dean at The University of Faisalabad, Pakistan. He is also the Head of the Network Communication and Media Analytics Research Group, National Textile University. He has authored two book chapters and has published over 100 research articles in prestigious journals. He has been engaged in many national- and international-level projects. He is on collaborative research with renowned research centers and institutes around the globe on various issues in the domains of the IoT, WSN, and blockchain. He is a Guest Editor of special issues in leading journals of his domain. He is also engaged as a TPC member/chair in many conferences. He is also a Guest Editor of IEEE ACCESS, *Concurrency and Computation Practice and Experience* (Wiley), *Future Generation Computer Systems* (Elsevier), *Peer-to-Peer Networking and Applications* (Springer), *Journal of Information and Processing System* (KIPS), *Cyber-Physical System* (Taylor & Francis), IEEE WIRELESS COMMUNICATIONS (IEEE Communication Society), and *IEEE Internet of Things Magazine*

Dr. Nabeel Asghar is serving as Assistant Professor at Bahauddin Zakariya University, Multan. He did his Degree in Doctor of Philosophy in the field of Computer Science from University of Bedfordshire, United Kingdom. He taught Data Structures, Object Oriented Programming, Introduction to Computing and Programming to undergraduate students and Managing student records, marking papers, preparing results. His research area is the Internet of Things, Information-Centric Networking, Ambient Intelligence, Wireless Sensor, Machine Learning, Databases, Data Science, Data Mining, Semantic Web, Social Media Analysis and Artificial Intelligence.

DR. UMAR RAZA is a Lecturer at Manchester Metropolitan University in Computer and Network technology. He received his PhD in Service Orientated Architecture (SOA) and Wireless Sensor Networks (WSN) approach applied to the measurement and visualization of a μInjection Molding Process from the University of Bradford Polymer IRC Laboratory. His previous experience includes seven years in the industry as a Software Engineer and over eight years of experience as a Lecturer in Robotics, Networking, and Computing at Staffordshire University. His current research interests and expertise include track and trace of pharmaceutical drugs using RFID and Blockchain technology, Industrial IoT data analytics and security, attribute-based authentication for IoT devices, data semantics and ontologies for Cyber-Physical systems. Application of machine learning in security, industrial, and assisted living fields using IoT devices.

Journal Pre-proof

Dr. Fadi Al-Turjman is a full professor and a research center director at Near East University, Nicosia, Cyprus. He is a leading authority in the areas of smart/intelligent, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation. His publication history spans over 250 publications in journals, conferences, patents and books. He serves as an associate editor and the lead guest editor for several international journals, including IET Wireless Sensor Systems.

Conflict of Interest

The All authors are declared that they have no conflict of Interest. The authors are certified that they have NO affiliations with or involvement in any organization or entity with any financial interest in the subject matter or materials discussed in this manuscript.

Journal Pre-proof