sustainability

MDPI

Article

A Content Poisoning Attack Detection and Prevention System in Vehicular Named Data Networking

Arif Hussain Magsi [1,2], Leanna Vidya Yovita [3], Ali Ghulam [2], Ghulam Muhammad [4,*] and Zulfiqar Ali [5]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; ahmagsi@bupt.edu.cn
[2] Information Technology Center, Sindh Agriculture University, Tandojam 70060, Pakistan; garahu@sau.edu.pk
[3] School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia; leanna@telkomuniversity.ac.id
[4] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[5] School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK; z.ali@essex.ac.uk
* Correspondence: ghulam@ksu.edu.sa

Abstract: Named data networking (NDN) is gaining momentum in vehicular ad hoc networks (VANETs) thanks to its robust network architecture. However, vehicular NDN (VNDN) faces numerous challenges, including security, privacy, routing, and caching. Specifically, the attackers can jeopardize vehicles' cache memory with a Content Poisoning Attack (CPA). The CPA is the most difficult to identify because the attacker disseminates malicious content with a valid name. In addition, NDN employs request–response-based content dissemination, which is inefficient in supporting push-based content forwarding in VANET. Meanwhile, VNDN lacks a secure reputation management system. To this end, our contribution is three-fold. We initially propose a threshold-based content caching mechanism for CPA detection and prevention. This mechanism allows or rejects host vehicles to serve content based on their reputation. Secondly, we incorporate a blockchain system that ensures the privacy of every vehicle at roadside units (RSUs). Finally, we extend the scope of NDN from pull-based content retrieval to push-based content dissemination. The experimental evaluation results reveal that our proposed CPA detection mechanism achieves a 100% accuracy in identifying and preventing attackers. The attacker vehicles achieved a 0% cache hit ratio in our proposed mechanism. On the other hand, our blockchain results identified tempered blocks with 100% accuracy and prevented them from storing in the blockchain network. Thus, our proposed solution can identify and prevent CPA with 100% accuracy and effectively filters out tempered blocks. Our proposed research contribution enables the vehicles to store and serve trusted content in VNDN.

Keywords: vehicular network; named data networking; blockchain; content poisoning attack

Citation: Magsi, A.H.; Yovita, L.V.; Ghulam, A.; Muhammad, G.; Ali, Z. A Content Poisoning Attack Detection and Prevention System in Vehicular Named Data Networking. *Sustainability* **2023**, *15*, 10931. https://doi.org/10.3390/su151410931

Academic Editors: Hoon Ko and Kiho Lim

Received: 2 May 2023
Revised: 6 July 2023
Accepted: 11 July 2023
Published: 12 July 2023

1. Introduction

The number of automobiles has skyrocketed globally in recent years. As a result of this unprecedented growth, issues such as car accidents and traffic congestion have been witnessed [1]. According to a projection in 2015, the number of traditional vehicles will double in the next 10 to 20 years [2]. The World Health Organization (WHO) predicts that road accidents will be the fifth leading cause of mortality by 2030 [3]. Alternatively, the vehicular ad hoc network (VANET) [4] has gained significant recognition to cope with road accidents and traffic congestion and facilitated drivers and passengers to obtain infotainment services.

Despite the impressive features and popularity of VANET, its communication mechanism has several limitations due to the end-to-end communication architecture of traditional transmission control protocol/internet protocol (TCP/IP). On top of its limitations, it is a

host-centric network that incurs additional overhead and exacerbates network latency [5]. In addition, security is the topmost priority in VANET, as human lives are directly involved in it.

To address TCP/IP limitations in VANET, today's internet paradigm has subverted the traditional host-centric network into a content-centric network. In this connection, named data networking (NDN) [6] is one of the most promising instances of an information-centric network (ICN) [7], which is envisioned as a future internet architecture. NDN has great potential to support high mobility, dynamic network topology, and intermittent connectivity, which makes NDN the most efficient network architecture for VNDN. Specifically, in-network content caching enables the consumer node to fetch the content from its vicinal replica node rather than querying a faraway original content provider. Another key feature of NDN is to secure content rather than the communication channel. In NDN, every data packet is signed with a cryptographic signature that guarantees packet security.

NDN was initially proposed by VAN Jacobson [8] under the U.S National Science Foundation (NFS) project. NDN employs two types of packets for content exchange, i.e., **Interest Packet**, which is used by consumers to express their desire for particular content in the network, and **Data Packet**, which contains a payload sent back to the content consumers. In addition, there are three types of nodes in NDN, i.e., **(1) Consumer Node**, which is a requester node that initiates an interest packet to fetch the content, **(2) Intermediate Node**, which is a relay node that forwards the content to the next hop; another role of the intermediate node is to cache the content in its local storage, and **(3) Producer Node**, which disseminates the content among content consumers or intermediate nodes using a data packet. NDN contains three data structures:

1. Content Store (CS): Each node maintains a CS to cache the received content. It provides the matched content to the consumer nodes rather than forwarding interest to the original content provider.

2. Pending Interest Table (PIT): A PIT keeps track of all the unsatisfied interests and their interfaces in a table.

3. Forward Information Base (FIB): The FIB determines name prefixes and forwards the interest packets to all available interfaces upstream except the incoming interface. The FIB is exploited when content is not satisfied by CS. Figure 1 depicts the content exchange mechanism of NDN in VANET.

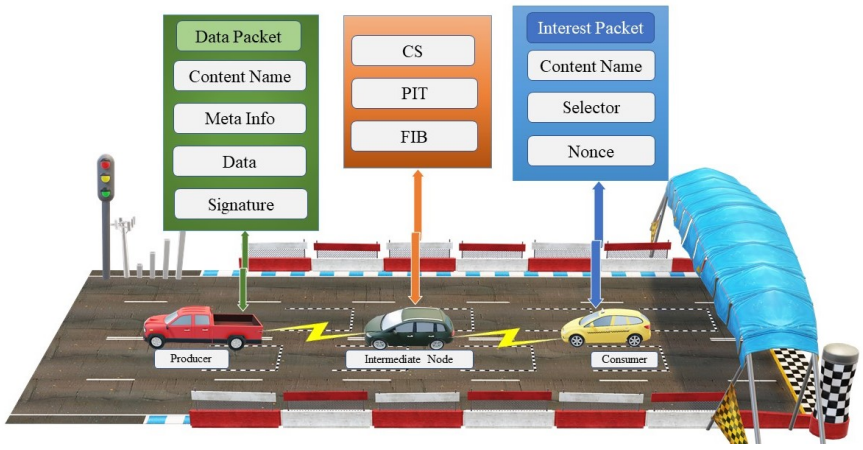

Figure 1. Content forwarding in VNDN.

Despite sprung-up features, the current form of NDN faces many challenges, including content forwarding, privacy, and security issues [9]. Specifically, NDN is highly vulnerable to a variety of attacks [10], including the Interest Flooding Attack (IFA) [11], Cache pollution Attack, [12], Man-in-the-Middle Attack [13], and Content Poisoning Attack (CPA). Among them, CPA is the most difficult to identify and prevent in VNDN because the attacker vehicles modify the original content with malicious data and distribute it with the correct name. In this connection, current literature has proposed several strategies, such as the

reputation management scheme [14], trust management scheme [15], and signature-based content legitimacy verification [16]. The authors of [17,18] proposed a blockchain-based reputation management scheme for secure content caching. Although these approaches are essential, they cannot adhere to the native content transmission scheme of NDN. Unlike the above-mentioned schemes, we propose a comprehensive network architecture for detecting and preventing CPA using a threshold-based reputation analysis at RSUs. Our proposed CPA detection mechanism classifies attackers and legitimate vehicles based on their previous reputation.

Another significant drawback of NDN is its pull-based content retrieval mechanism, where producer nodes are passive. They can only provide content once a content consumer node initiates an interest packet for a corresponding data packet. To enhance the scope of NDN from a pull-based content retrieval mechanism to a push-based content dissemination mechanism, we employ the Publish-Subscribe (Pub-Sub) [19] system for disseminating content among pre-subscribed nodes. We integrate pub-sub in our proposed reputation dissemination scheme for disseminating the reputations of host vehicles among RSUs in VNDN.

Meanwhile, secure reputation management is another challenge in VNDN. The centralized cloud-based [20] and distributed reputation management scheme [21] are inefficient in VANET due to the mobility of nodes. Blockchain is gaining momentum to maintain the reputation of vehicles securely due to its secure, distributed, and append-only characteristics. As illustrated in Figure 2, a blockchain contains a series of blocks. Each block is linked to another block. A block contains transactions, the previous block's hash, and a nonce (a random or incremental number used in blockchain mining to find a hash that meets specific criteria). Leveraging the properties of blockchain, numerous research contributions have been made in the last decade; for example, the authors of [21–26] proposed different blockchain strategies for secure data storage in VANET. However, none of those mentioned above explored the blockchain system for CPA detection in VNDN.

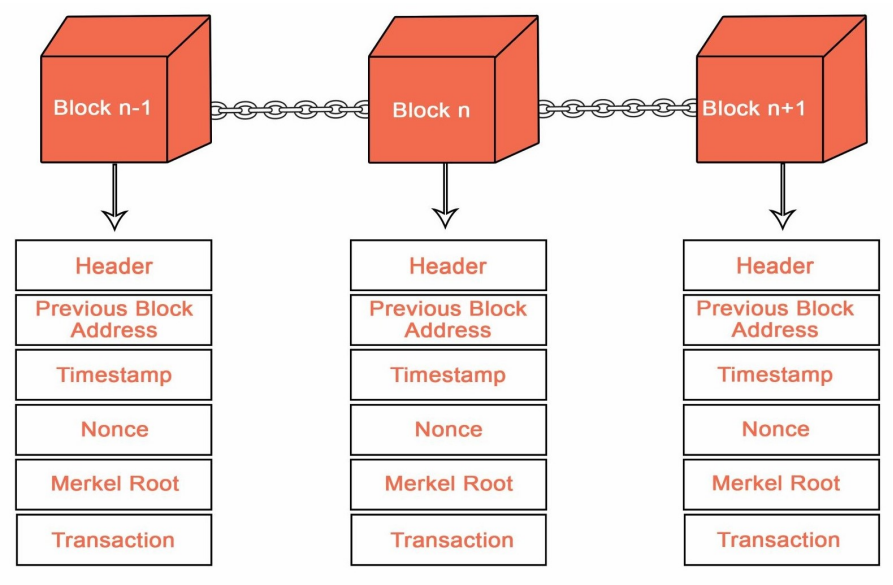

Figure 2. Blockchain block structure.

Keeping in view the challenges mentioned above and considering the limitations in existing literature, the fundamental goal of this research is to propose an effective network framework for valid content dissemination and CPA detection and prevention system using a reputation management scheme. Thus, our proposed research work prevents intermediate vehicles from accepting malicious content from attacker vehicles. The key contributions of this research are as follows:

- We evaluate the legitimacy of vehicles using a threshold-based reputation management system that classifies vehicles as attacker or benign.
- We propose push-based content dissemination in VNDN that enables vehicles to propagate content without considering interest packets.
- We integrate a blockchain-based reputation management system that stores the reputation of every vehicle at RSUs.

The remainder of this paper is organized as follows. In Section 2, we review the related works for efficient content caching and CPA detection in VNDN and highlight their limitations. Section 3 discusses a detailed system model, network elements, and a proposed network architecture. We provide implementation details and simulation results in Section 4. Finally, Section 5 provides a conclusion and suggestions for future work.

2. Related Work

Although the concept of enhancing security in VNDN is widely acknowledged [27], the development and implementation of effective measures to prevent security attacks [28] in VNDN is still in its early stage. The strategies for efficient content caching include popularity-based content caching [29,30], cooperative caching [31], signature-based content verification [32], and rating-based trust management system [21].

Most recent work in [33] integrated blockchain into NDN for a secure and trusted content caching scheme in VNDN. The authors evaluated the legitimacy of the content and assigned them positive or negative ratings. This work derived an algorithm based on a biological rule named the honeyGuide search algorithm. In this system, each node is assigned an initial ranking that is updated according to the behavior of the content-providing node. The authors also proposed a Malicious Vehicle Table (MVT) containing a list of CPAs. The nodes query the MVT before caching content. On the other, signature-based content legitimacy verification is exploited in [32]. In this approach, the content consumer verifies the signature of the host node by querying another node. The authors of [34] proposed a Most Frequently Requested Content (MFRC) scheme that caches frequently requested content.

Analogously, Khelifi et al. [35] proposed a blockchain-based reputation system for CPA detection and prevention system in VNDN that evaluates the reputation of every content provider before caching their content in CS. Additionally, the authors improved and extended research in [17]. They proposed a blockchain-based reputation system that addresses both IFA and CPA. Their latest research work evaluates the reputation of content consumers and producers. Thus, this research mitigates the IFA by calculating the total interest sent, total PIT size, and average expunge time of PIT entry. Based on these calculations, the reputation of content consumers is determined and stored in a Local Neighbors Table (LNT). Secondly, the proposed mechanism mitigates CPA by evaluating the reputation of CS.

In [36], Kim et al. proposed an optimized fuzzy reputation-based trust model for detecting and preventing CPA at the intermediate node in NDN that saves computational resources and flushes out the invalid content from CS. Another significant contribution [37] employed a blockchain-based secure content sharing scheme in VNDN, wherein a double-layer blockchain content sharing was proposed. In the bottom layer, all the nodes are specified in a group with the same interests. The nodes in a group can desire the content of their interest within the group. If no content is available in the relevant group, the request is forwarded to the upper layer of RSUs. Each group maintains its own blockchain and mining process. Moreover, the authors proposed an incentive-based reputation management system that records positive and negative reputations through blockchain transactions.

Lei et al. in [38] integrated a private blockchain to maintain Unmanned Aerial Vehicles (UAV) information in NDN. This study aims to exploit blockchain to cope with CPA by verifying the content name and publisher key digest. The authors employed a consensus algorithm named adaptive delegate consensus algorithm (ADCA), a lightweight consensus algorithm that does not require a mining process. In [39], Bernardini et al. proposed a Most

Popular Content (MPC) strategy for caching the most popular content in CS. The content popularity relies on the cache hit ratio. The more hits for content is considered reputable content. In this scheme, every node maintains a popularity table comprising the content name and popularity score, which relies on a pre-defined threshold.

Similarly, Yang et al. in [23] designed a blockchain-based reputation system for assessing the credibility of content in VANET. This work issues the ratings to the content-providing vehicles, which are then forwarded to a temporarily selected node as blocks. The temporarily selected node is responsible for propagating the reputation among other nodes. Similar to our work, ref. [40] proposed reputation-based content dissemination in VANET, wherein the reputation of a host vehicle is evaluated before acting upon the message. In this work, reputation is stored and aggregated by a trusted centralized authority. Finally, the authors of [41] proposed a content source verification for multiple receivers. In this scheme, every consumer node verifies the signature of the content producer. However, the content producer can inject malicious content with the correct signature. Thus, the proposed approach cannot verify the legitimacy of the content. Table 1 reflects the limitations of the above-mentioned related work.

Table 1. Summarized related works and their limitations.

References	Architecture	Scheme	Limitations
Sabir et al. [33]	VNDN	Rating-based content caching	The proposed work lacks rating dissemination among blockchain nodes.
Ullah et al. [32]	NDN	Signature-based CPA detection	This approach verifies the legitimacy of every content by querying the signature. However, it cannot verify the signature of new content that has not been previously served.
Naeem et al. [34]	NDN	Popularity-based content caching	This caches frequently requested content. However, attackers can compromise the CS of intermediate nodes with unpopular content.
Khelifi et al. [35]	VNDN	Reputation-based push content caching	Although the authors significantly contributed to addressing CPA and IFA, they could not follow the native architecture of NDN communication,
Kim et al. [36]	NDN	Reputation-based trust model	The authors evaluated the reputation of every node. This mechanism ignored the reputation evaluation and dissemination mechanism.
Chen et al. [37]	VNDN	Blockchain-based content sharing scheme	This scheme did not consider the reputation-based content caching mechanism in intermediate nodes.
Lei et al. [38]	UAV NDN	Signature-based reputation verification	The signature verification for every content introduces an additional delay.
Bernardini et al. [39]	NDN	Content popularity	The content popularity scheme is at high risk of attackers where they can express interest in unpopular content and make it popular with frequent interest requests.
Yang et al. [23]	VANET	Rating-based content dissemination	The rating-based content dissemination in VANET is different from the VNDN architecture.
Li et al. [40]	VANET	Reputation-based announcement scheme	The proposed scheme allows RSUs to store reputation. However, attackers can compromise a centralized authority, which can result in an amendment to the reputation score of vehicles.
Hussain et al. [41]	NDN	Signature-based content verification	The proposed mechanism verifies the signature at every consumer node. However, an attacker can inject fake content with the correct signature.

The above-mentioned related works provide a partial and traditional solution to mitigate CPA. Unlike those works, our proposed work provides an intelligent CPA detection and prevention mechanism that categorizes vehicles into three categories. These categories are reputed vehicles, legitimate vehicles, and attacker vehicles. Based on the category of vehicles, our proposed algorithm decides to accept or reject the hosted content. Secondly, our proposed blockchain-based reputation management scheme ensures the security and privacy of every vehicle's reputation. Finally, we enhance the scope of NDN from push-based content retrieval to push-based content dissemination. Table 2 shows the notations used in this paper.

Table 2. Summary of notations.

Notation	Description
I_Pkt	Interest Packet
D_Pkt	Data Packet
C_P	Content Producer
C_C	Content Consumer
CP_R	Content Producer Reputation
C_R	Content Reputation
T_C	Trusted Content
CP_R^n	Content Producer New Reputation
$CP_R^n - 1$	Content Producer Previous Reputation
$AgrCP_R$	Aggregate Content Producer Reputation

3. System Model

This section exhibits the major entities and their roles in our proposed system model. In this section, we propose a content caching mechanism for detecting and preventing CPA in accordance with our proposed Algorithm 1. Then, we propose a content validation scheme at the content consumer node, as per Algorithm 2. Thereafter, we propose push-based transaction dissemination among RSUs using a suitable naming structure. Furthermore, this section proposes a blockchain block propagation and verification scheme.

3.1. System Components

As depicted in Figure 3, the proposed system comprises several essential components with distinct roles, as mentioned below:

Trusted Authority (TA): TA is responsible for registering the vehicle by assigning them a pair of keys (public and private).

Car: An OBU-equipped car can serve as a consumer, intermediate node, or producer, with interchangeable roles depending on the situation.

RSU: Keeping in view the availability and stability of RSUs alongside the road, their primary role is to calculate, store, and provide the aggregate reputation of every vehicle to the requesting nodes. In addition to RSUs, we determine public buses as moving RSU (mRSU) [42,43]. Due to their mobility and prolonged availability, they are suitable to provide reputations to the vehicles.

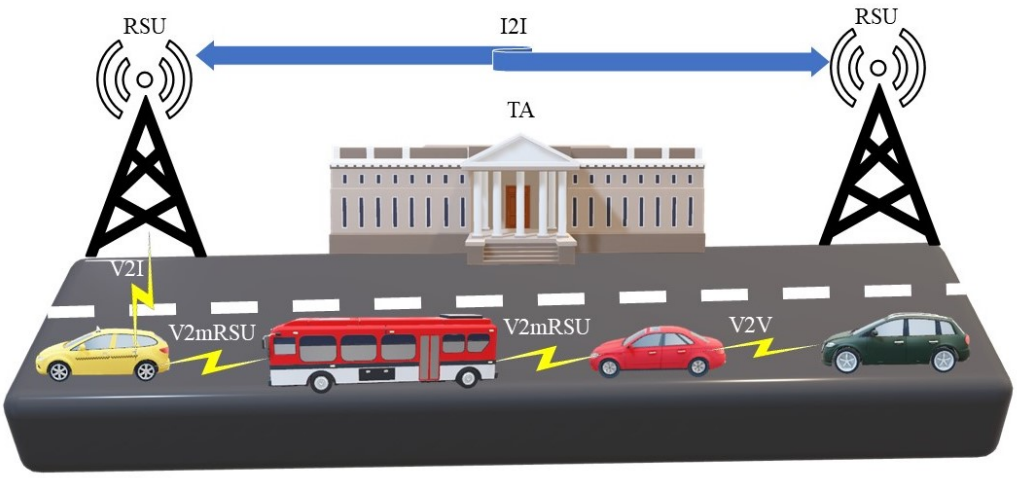

Figure 3. System components in VNDN.

3.2. Secure Content Caching Mechanism

Our proposed content caching mechanism aims to identify and prevent attacker vehicles. We enable RSUs to evaluate every vehicle's threshold-based reputation to achieve our goal. Unlike the default content caching mechanism of NDN, which allows intermediate nodes to store every content at intermediate nodes without determining content legitimacy, we first evaluate the legitimacy of the content-providing node before caching served content in CS. Based on our proposed reputation evaluation, an intermediate node decides whether to cache or ignore the content provided by a producer. In our proposed Algorithm 1 and Figure 4, an intermediate node receives an interest packet from a content consumer and forwards it to the content producer. The content producer then serves the requested content with a data packet to the intermediate node. Subsequently, the intermediate node queries its local reputation data. It is worth noting that every node must download an updated reputation of a host vehicle from RSUs. Due to the mobility of nodes, the intermediate nodes cannot query RSUs/mRSUs during content transmission. Therefore, each vehicle must receive an updated aggregated reputation of all the vehicles from RSUs/mRSUs using an optional "MustBeFresh" field in the interest packet. Our content caching decision is based on three rules. (1) Cache and forward the content to the consumer if the reputation score of the host vehicle is greater than 10. (2) Forward the content to the consumer without caching it if the reputation score is between 0 and 9. (3) Immediately discard the packet if the reputation score is negative. Following our content caching policy, the intermediate node decides whether to cache, forward, or discard the data packet. Our reputation-based scheme initially assigns a 0 reputation score to every newly joined node. In our proposed reputation management system, the role of RSUs/mRSU is to collect and calculate the reputation of every individual vehicle and provide an aggregate reputation according to Equation (1). The aggregate reputation score enables the intermediate nodes to classify CPA and legitimate nodes:

$$CP_R^n = \frac{\sum CP_R}{n} \tag{1}$$

where CP_R denotes the number of calculated reputations of a content producer and is assigned to CP_R^n, which represents the aggregate reputation score of a producer node. Thus, no content sent from CPA will be stored in the CS of the intermediate node or forwarded to the content consumer node.

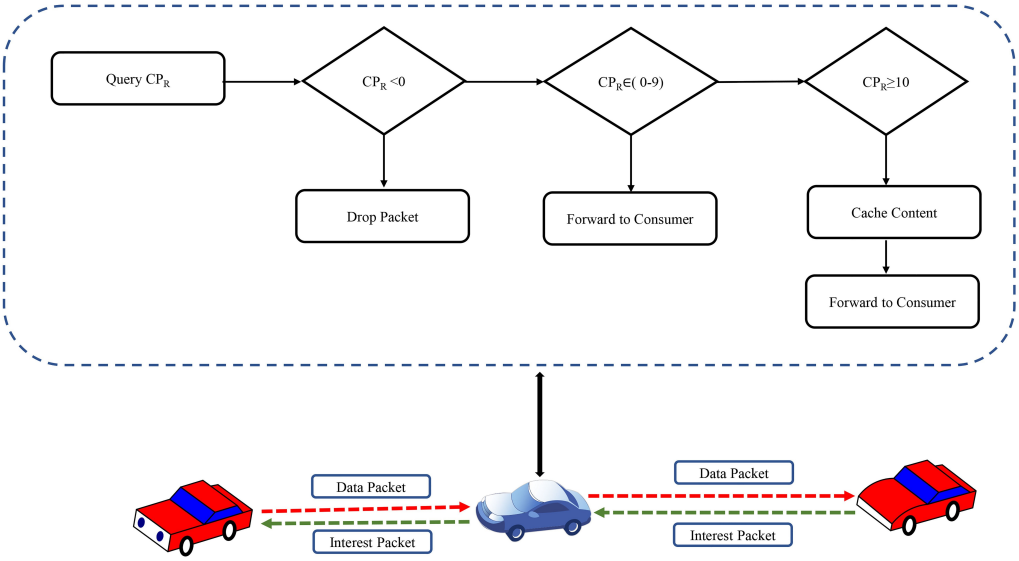

Figure 4. Content caching policy.

Algorithm 1 Content Caching policy at the intermediate node

Require: *DataPacket* from *ContentProducer*

Calculate (1)
if $CP_R < 0$ **then**
    Drop the packet
else if $CP_R \in (0, 9)$ **then**
    Forward Data Packet to Content Consumer
else if $CP_R \geq 10$ **then**
    Cache content
    Forward Data Packet to Content Consumer
end if

Our proposed Algorithm 1 determines a pre-configured threshold-based reputation system. In this system, a threshold-qualifying vehicle with a reputation score of (10) or above is considered reputed. An intermediate node caches and forwards the content to the consumer node if the content provider is reputed. On the other hand, a vehicle with a reputation value between 0 and 9 is considered trusted. Their hosted content can be forwarded to the consumer without caching at the intermediate node because they are not yet qualified for content caching. Finally, we assume a vehicle is an attacker with a negative reputation.

3.3. Content Validation Mechanism

Upon receiving content from the intermediate node, the content consumer utilizes and evaluates the legitimacy of the content. The content validation policy plays a significant role in this stage. Based on the legitimacy of content, the content consumer node decides whether the served content is valid or malicious. According to Equation (2), legitimate content is identified with 1 and malicious content with 0. In our proposed content validation scheme, a consumer rewards a producer (x) with +1 if the served content is valid. Conversely, a producer (x) is punished with -1 if the served content is malicious/invalid. After assigning the reputation value $f(x)$ based on the legitimacy of the content, a consumer has another role in broadcasting the reputation of the content producer among pre-subscribed RSUs/mRSUs. Algorithm 2 shows the content validation and transaction dissemination

among RSUs/mRSUs. It is worth noting that consumers can identify the content producers with their public key assigned by TA.

$$f(x) = \begin{cases} x+1, & x = 1 \\ x-1, & x = 0 \end{cases} \quad (2)$$

Algorithm 2 Content validation policy

Require: Data Packet
1: **if** *DataPacket=Trusted* **then**
2: $CP_R^n \leftarrow CP_R^{n-1} + 1$
3: Push CP_R^n to pre-subscribed vehicles
4: **else if** $CP_R \neq$ Trusted **then**
5: $CP_R^n \leftarrow CP_R^{n-1} - 1$
6: Push CP_R^n to pre-subscribed vehicles
7: **end if**

3.4. Pub-Sub Model

In our proposed system model, we enable the nodes to broadcast the reputation of host vehicles without receiving interest requests for each content. To this end, we exploit a pub-sub in VNDN. The proposed pub-sub model allows consumer nodes to disseminate the reputation score (+1 or −1) to the nearest RSUs/mRSUs. It is important to note that every RSU/mRSU must subscribe to the reputations at least once using a prefix naming structure, e.g., */VNDN/Reputation/Version/MustBeFresh*. The naming structure for the subscription of a reputation informs the nodes to send back the latest reputation of vehicles when it becomes available. In the response, a publisher (which is the consumer in NDN) provides the content producer's reputation with the naming structure *VNDN/Reputation/Version/Vehicle/No/(+1 or −1)*. Our proposed scheme prevents subscribing to every vehicle's reputation individually. Due to the unpredictable reputation generation time, it is infeasible for subscribers to decide when to broadcast the subscription packet for a specific reputation. Periodic subscription requests that are too short or too long can impact network performance. Therefore, we design a suitable prefix naming structure that enables the RSUs/mRSUs to receive many packets in response to a single subscription request.

3.5. Naming Structure

The opaque naming structure plays a significant role in content dissemination in NDN. It allows the applications to design the naming structure as per requirement. Taking advantage of the flexible naming structure and considering the native hierarchical naming rule of NDN, we propose the following naming structure for interest packet requests, reputation requests to RSUs/mRSUs, and subscription requests in pub-sub.

Content Request: */VNDN/Infotainment/Misuc/Artist/Album/Track*
Reputation Request: */VNDN/Reputation/Version/MustBeFresh*
Subscription Request: */VNDN/Pub-Sub/Reputation/MustBeFresh*

3.6. Transaction and Block Dissemination

Leveraging the availability of RSUs/mRSU on the road, we consider them blockchain nodes in our proposed system. Their primary role is receiving transactions from vehicles and storing and sharing them in the network. To disseminate the reputation of vehicles among blockchain nodes, the content validator (consumer) takes advantage of pub-sub and broadcasts the reputation (+1 or −1) in the form of a blockchain transaction to the nearest RSU/mRSU. Once RSU/mRSU receives the transaction, it packs the transaction into a block and disseminates it among all blockchain nodes. Subsequently, every blockchain node receives and performs a specific consensus algorithm (mining) to validate the block, as shown in Figure 5.

3.7. Consensus Mechanism

The consensus mechanism plays a significant role in validating the blocks in the blockchain. It ensures that all nodes in the network agree to append the block to the network. Thus, the consensus mechanism prevents tempered blocks from appending in the blockchain. After creating and disseminating the block to the blockchain network, our proposed consensus mechanism takes place to validate the block. Our proposed system uses the PoW consensus mechanism, which is the most secure and difficult for attackers to manipulate. PoW requires the nodes to perform complex calculations to mine the block. In the blockchain, the attacker nodes can compromise the integrity of RSUs/mRSU with propagating tempered blocks by changing or deleting transaction data. To verify the integrity of blocks, the blockchain nodes calculate the previous block's hash. Any change in the hash of the previous block will automatically reject the block. Hence, adding a tempered block to the blockchain network is nearly impossible.

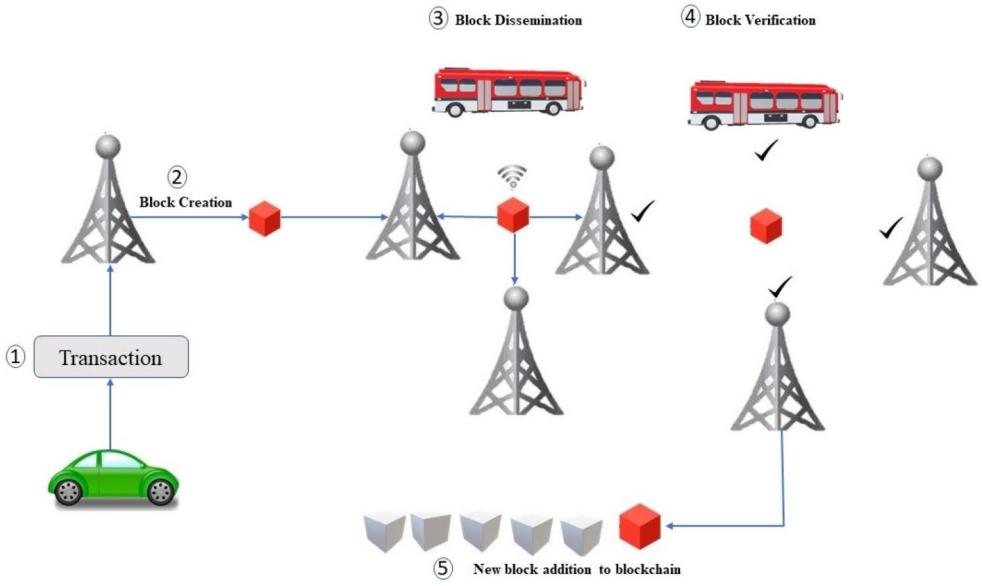

Figure 5. Block generation and dissemination.

3.8. A Summarized System Model Flow

As illustrated in Figure 6, our proposed system model flowchart exhibits content dissemination, content caching, content validation, reputation propagation, and block validation in the blockchain. Our proposed model is divided into four stages. Stage 1: A content consumer node broadcasts an interest packet to the intermediate node. The neighboring intermediate node satisfies the interest request if the corresponding information is available in its CS. Otherwise, the intermediate node forwards the request to other nodes. A node with matched content responds with a data packet to the intermediate node. Step 2: Before caching content in its CS or forwarding it to the consumer, the intermediate node evaluates the reputation of the content producer. Based on the reputation score, an intermediate node decides whether to cache, forward, or reject the content. Step 3: The content consumer uses and classifies the content as legitimate or malicious. Based on this evaluation, the consumer node assigns (+1 or −1) and propagates the reputation as a transaction to the blockchain network. Step 4: The blockchain nodes receive the transaction, pack it into the block, and disseminate it among neighboring nodes. The neighboring nodes apply the PoW consensus algorithm. Based on the legitimacy of the block, the nodes add a valid block or reject a tempered block.

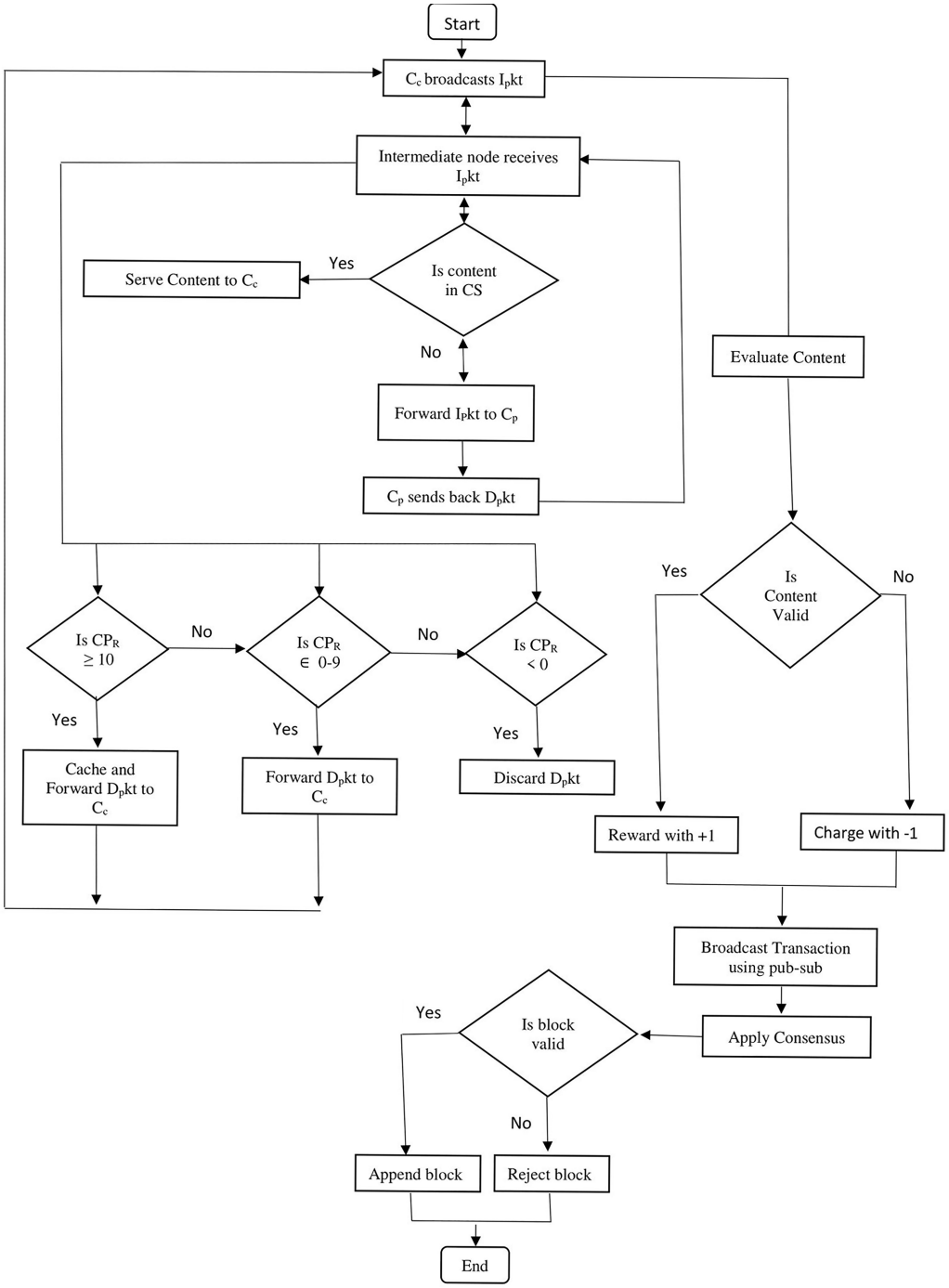

Figure 6. Overall system model flowchart.

4. Simulation-Based Evaluation

We divided our experimental evaluation into two parts. Initially, we evaluated the performance of our proposed threshold-based reputation evaluation algorithm for detecting and preventing CPA. Secondly, we evaluated the performance of our blockchain architecture to ensure secure reputation management. To evaluate the effectiveness of our proposed CPA detection scheme, we simulated our experimental evaluation in a MATLAB simulation. As mentioned in Table 3, our simulation involves attacker and legitimate host vehicles with static reputation values. In addition, we used Javascript to evaluate the integrity of the blockchain network. Our proposed blockchain-based attack detection mechanism initially stores the reputation of every vehicle in a secure and distributed ledger at RSUs.

The RSUs then aggregate the reputation of every vehicle according to (1). The blockchain simulation evaluates the legitimacy of blocks and allows or prevents nodes from adding to the blockchain network. We simulated our MATLAB and javascript simulation on an Intel Desktop Core i-7 CPU at 2.8 GHz, with 16 GB RAM on the Windows 11 operating system. In MATLAB simulation, we considered cache placement decisions based on the threshold reputation value of every content producer. Our proposed architecture aims to allow reputation-qualifying vehicles to send their content and prevent attacker vehicles from serving intermediate nodes. On the other hand, our blockchain results identified the tempered blocks and did not store them on the blockchain network.

Table 3. Parameter settings.

Parameters	**Values**
Total Nodes	10
Producers	4
Intermediate Nodes	1
Content Consumers	5
Malignant Nodes	2
Benign Nodes	2
Request Pattern	Zipf Mandelbrot Distribution
Unique Contents	100
Exponential Factor	0.8, 1, and 1.2
Content Storage Size	5, 10, 15 Packets
Flattened Factor	3
Simulation Time	50 s
Interest rate	Average = 100 Interest for each consumer in one round, following the Zipf Mandelbrot.

4.1. Reputation Evaluation

Our proposed reputation evaluation algorithm performs a threshold-based decision system at the intermediate node. The reputation of every content-producing node and cache placement decision is made using MATLAB simulation. The simulation follows the Zipf-Madelbrot distribution for sending interest packets. The average number of unique interest packets each consumer sends is 100 messages. We repeated every simulation scenario three times and calculated their average. As depicted in Table 4, our proposed scheme contains benign and malignant producers. Both types of nodes respond with a data packet to the intermediate node. Correspondingly, the intermediate node queries its local reputation table, which was previously received from RSU/mRSU. Based on the aggregate reputation score, the intermediate node stores and forwards the data packet to the consumer if the host vehicle has an aggregate reputation score greater than 10. In another situation, the intermediate node forwards the content to the consumer without caching if the reputation score is between 0 and 9. Finally, the intermediate node rejects the content if the host has a negative reputation. The simulation parameters of our experimental evaluation are mentioned in Table 4.

Table 4. Nodes with their reputation score.

Node	Reputation Score
Producer-1	12
Producer-2	−5
Producer-3	−2
Producer-4	15

We assign a fixed aggregate reputation to every content-producing vehicle in our proposed content caching mechanism, as illustrated in Table 3. This reputation score is based on the vehicle's historical reputation. We modeled the request pattern on Zipf Mandelbrot, where nodes can cache the content locally. By incorporating local caching into our model, we can evaluate the impact of caching strategies on overall system efficiency and effectiveness and identify critical factors that contribute to optimal caching performance. We designed our system to allow nodes to cache content locally, which can help to improve overall system performance by reducing the need for content fetched from remote servers. The flattened factor in our proposed simulation enables the nodes to prioritize top-ranked content providers over low-ranked ones. Equation (3) expresses the probability of accepting the content, where we calculate the probability of the data packet P(d) and the number of content requests (d + q).

$$p(i) = \frac{(d+q)^{-\alpha}}{\sum_{d=1}^{N}(d+q)^{-\alpha}} \tag{3}$$

We denote "cache hit (h)" as the number of data packets received from the producer, and "missed hits (m)" represent the ignored packets at the intermediate node. Furthermore, the "cache hit ratio (THR)" depicts the successfully cached data packets:

$$THR = \frac{h}{h+m} \tag{4}$$

We tested default NDN content caching and our proposed reputation-based content caching three times and calculated their average hit ratios. We evaluated and compared the performance of our proposed scheme with the NDN default content caching system on various CS sizes (5, 10, and 15). To compare our proposed model with the default content caching strategy of NDN, we initially performed a MATLAB simulation on simple NDN. The experimental results reveal that every producer (P1 to P4) hits the CS of the intermediate node without any verification. In contrast to the default content caching strategy, our proposed reputation-based CPA mitigation system evaluates the reputation of every node first and decides whether to hit the cache or discard the packet. In our proposed model, both P2 and P3 have a negative reputation, as mentioned in Table 3. Therefore, they achieved a 0% hit ratio. Hence, every malignant node with a negative reputation will be immediately discarded. The CS hit ratio in all the configurations exhibits the superiority of our proposed content caching mechanism over the default content caching system. In particular, the CS size 15 shows the highest THR, as shown in Figure 7. Moreover, as depicted in Figure 8, we tested the THR on different exponential factors similar to the cache hit ratio, which shows that the attackers nodes (producer 2 and 3) achieved a 0% hit ratio on exponent factors 0.8, 1, and 1.2. However, the default NDN allowed P2 and P3 to hit the cache.

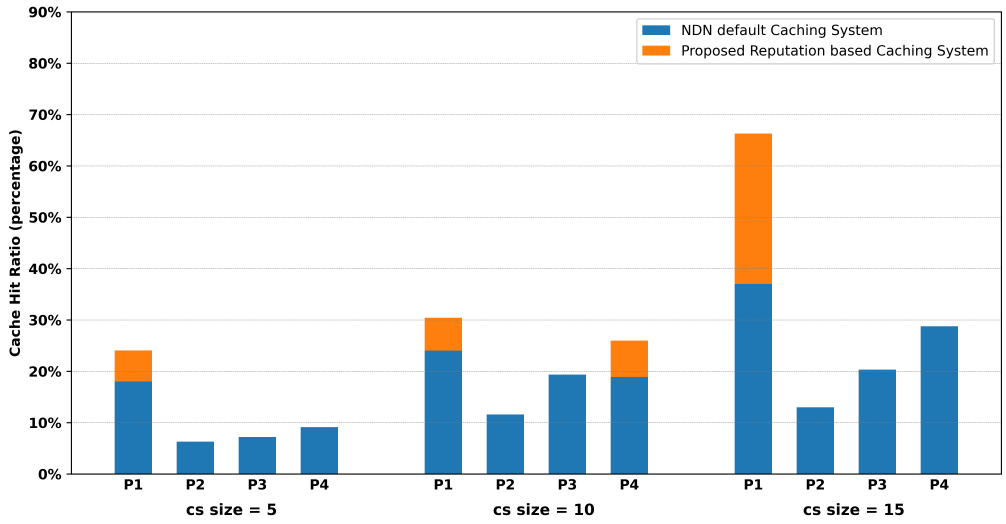

Figure 7. Cache hit ratio using various CS sizes.

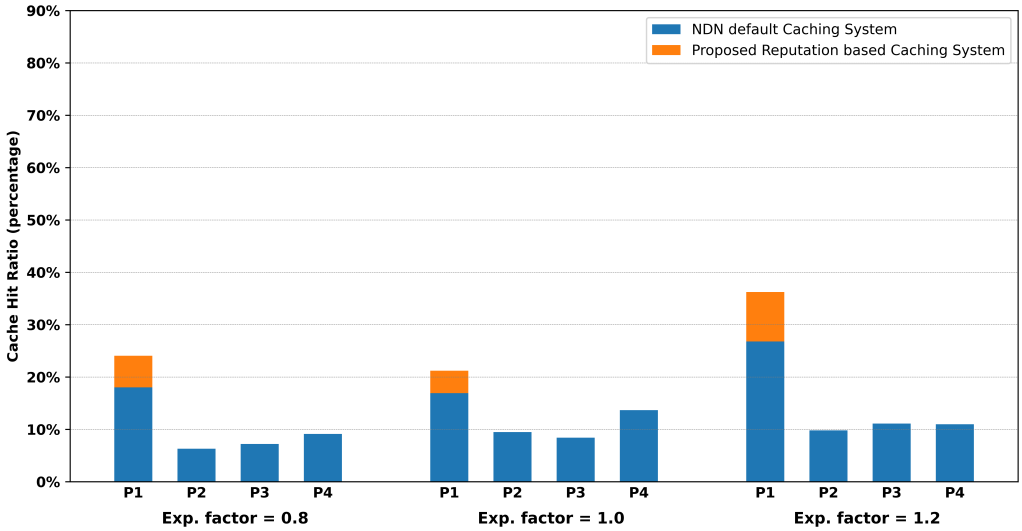

Figure 8. Cache hit ratio using various exponential factors of Zipf Mandelbort.

The achieved results reflect the accuracy of our proposed CPA detection and prevention system, where the attacker vehicles achieved a 0% hit ratio. The results mentioned in Figures 7 and 8 compare the default NDN content caching hit ratio with our proposed scheme. In the default caching mechanism of NDN, the intermediate nodes accept every issued data packet without considering the legitimacy of the content provider. On the other hand, the intermediate vehicles cache content from reputed vehicles and rejects the content of negative reputation-holding vehicles using our proposed content caching algorithm. Thus, our proposed reputation-based CPA detection and prevention mechanism trusts reputed vehicles and neglects attacker vehicles. Meanwhile, we tested the computational time of our proposed model that is equal to the simulation time, as mentioned in Table 3.

4.2. Blockchain Security Analysis

To ensure privacy and security, blockchain has a significant role in managing the reputation of every individual vehicle in a distributed and secure digital ledger. In our blockchain integrity verification system, we used Javascript to create blocks, implemented a consensus mechanism, and analyzed the design and implementation of our proposed model. The proposed blockchain architecture consists of ten blocks, three of which are

intentionally tampered with respect to the transaction values. To evaluate the effectiveness of our approach, we propagated both legitimate and tempered blocks throughout the network. Our proposed mechanism used a binary code to differentiate between tampered blocks (indicated with a 0) and legitimate blocks (indicated with a 1). As shown in Figure 9, all the blocks were successfully verified and stored in the blockchain. However, tempered blocks (3, 6, and 9) were rejected due to changes in the hash value. Our blockchain integrity verification system aims to prevent compromised RSUs/mRSUs from gaining control over the blockchain and tampering with it.

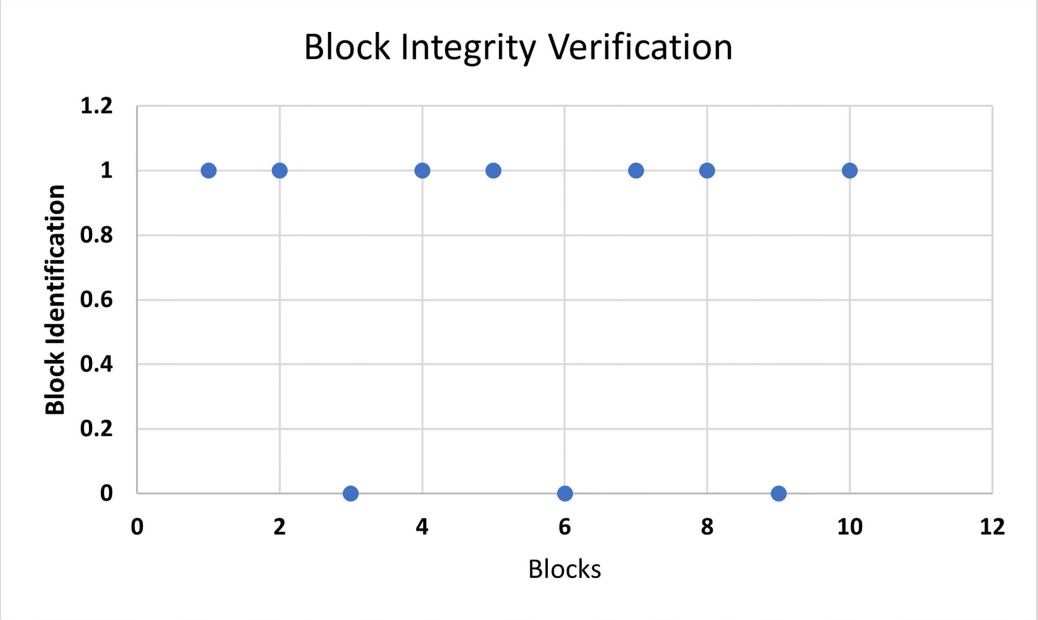

Figure 9. Blockchain integrity verification.

5. Conclusions

The NDN in VANET faces several challenges, including security, privacy, and fair content dissemination. Specifically, secure content dissemination is an extremely important facet of VNDN, where the existence of CPA can jeopardize the integrity of the whole network. To solve the above-mentioned challenges, we proposed a threshold-based CPA detection and prevention technique. In this paper, we address CPA, ensure privacy, and enhance the scope of NDN from pull-based content retrieval to push-based content dissemination. Our proposed CPA detection scheme enables intermediate nodes to accept or reject the content based on the reputation of vehicles. Thus, our proposed model motivates legitimate vehicles to exchange trusted content and reject malicious content. We compared our proposed scheme with default content caching in NDN, reflecting that our proposed mechanism identifies attackers with 100% accuracy. On the other hand, the default NDN caching mechanism stores every content without determining the legitimacy of the content provider. Besides, we integrated a decentralized and secure blockchain system to store the reputation of every vehicle at RSUs/mRSUs. Our proposed blockchain-based framework stores all privacy content and prevents attackers from tempering with the blocks with 100% accuracy. Finally, we enhance the scope of NDN using a pub-sub mechanism that enables nodes to disseminate reputation through push-based communication. Hence, our contribution significantly enhances confidence among vehicles to accept or reject content based on the reputation of content-providing vehicles. Moreover, the scope of this research is limited to simulation-based CPA detection and prevention, which can be further executed in an NDN testbed using real-time scenarios. Our proposed CPA detection system is a rule-based reputation evaluation system. The CPA detection system can be further evaluated in future work through Machine Learning (ML) and Deep Learning (DL) classifiers using different publicly available datasets. Thus, the most accurate classifier can detect

CPA with accuracy. Moreover, our proposed research work is simulation-based, which can be further implemented in real-time scenarios in the future.

Author Contributions: Conceptualization, A.H.M. and L.V.Y.; methodology, A.H.M., A.G. and G.M.; software, A.H.M., L.V.Y., A.G. and Z.A.; validation, L.V.Y., A.G. and Z.A.; formal analysis, L.V.Y. and Z.A.; investigation, L.V.Y., A.G. and Z.A.; resources, A.H.M. and G.M.; data curation, G.M.; writing—original draft, A.H.M., G.M. and Z.A.; Writing—review and editing, G.M.; visualization, A.H.M. and A.G.; funding acquisition, G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Research Supporting Project Number: (RSP2023R34), King Saud University, Riyadh, Saudi Arabia.

Acknowledgments: The authors acknowledge the Researchers Supporting Project number (RSP2023R34), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, H.; Qiu, T.; Zhou, X.; Chen, C.; Chen, N. Parking-Area-Assisted Spider-Web Routing Protocol for Emergency Data in Urban VANET. *IEEE Trans. Veh. Technol.* **2020**, *69*, 971–982. [CrossRef]
2. Jia, D.; Lu, K.; Wang, J.; Zhang, X.; Shen, X. A survey on platoon-based vehicular cyber-physical systems. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 263–284. [CrossRef]
3. Sun, L.; Lin, Z.; Li, W.; Xiang, Y. Freeway incident detection based on set theory and short-range communication. *Transp. Lett.* **2019**, *11*, 558–569. [CrossRef]
4. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]
5. Naeem, M.A.; Rehman, M.A.U.; Ullah, R.; Kim, B.S. A comparative performance analysis of popularity-based caching strategies in named data networking. *IEEE Access* **2020**, *8*, 50057–50077. [CrossRef]
6. Zhang, L.; Afanasyev, A.; Burke, J.; Jacobson, V.; Claffy, K.; Crowley, P.; Papadopoulos, C.; Wang, L.; Zhang, B. Named data networking. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 66–73. [CrossRef]
7. Xylomenos, G.; Ververidis, C.N.; Siris, V.A.; Fotiou, N.; Tsilopoulos, C.; Vasilakos, X.; Katsaros, K.V.; Polyzos, G.C. A survey of information-centric networking research. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1024–1049. [CrossRef]
8. Jacobson, V.; Smetters, D.K.; Thornton, J.D.; Plass, M.F.; Briggs, N.H.; Braynard, R.L. Networking named content. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, Rome, Italy, 1–4 December 2009; pp. 1–12.
9. Safwat, M.; Elgammal, A.; AbdAllah, E.G.; Azer, M.A. Survey and taxonomy of information-centric vehicular networking security attacks. *Ad Hoc Netw.* **2022**, *124*, 102696. [CrossRef]
10. Shah, M.S.M.; Leau, Y.B.; Anbar, M.; Bin-Salem, A.A. Security and Integrity Attacks in Named Data Networking: A Survey. *IEEE Access* **2023**, *11*, 7984–8004. [CrossRef]
11. Benmoussa, A.; Kerrache, C.A.; Lagraa, N.; Mastorakis, S.; Lakas, A.; Tahari, A.e.K. Interest Flooding Attacks in Named Data Networking: Survey of Existing Solutions, Open Issues, Requirements, and Future Directions. *ACM Comput. Surv.* **2022**, *55*, 1–37. [CrossRef]
12. Hidouri, A.; Hadded, M.; Hajlaoui, N.; Touati, H.; Muhlethaler, P. Cache pollution attacks in the NDN architecture: Impact and analysis. In Proceedings of the 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 23–25 September 2021; pp. 1–6.
13. Mallik, A. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace J. Pendidik. Teknol. Inf.* **2019**, *2*, 109–134. [CrossRef]
14. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks. *IEEE Access* **2017**, *5*, 25408–25420. [CrossRef]
15. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, E. Information-oriented trustworthiness evaluation in vehicular ad hoc networks. In Proceedings of the International Conference on Network and System Security, Madrid, Spain, 3–4 June 2013; pp. 94–108.
16. Huang, H.; Wu, Y.; Xiao, F.; Malekian, R. An efficient signature scheme based on mobile edge computing in the NDN-IoT environment. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 1108–1120. [CrossRef]
17. Khelifi, H.; Luo, S.; Nour, B.; Moungla, H.; Guizani, M. A Blockchain-based Architecture for Secure Vehicular Named Data Networks. *Comput. Electr. Eng.* **2020**, *86*, 106715. [CrossRef]

18. Li, X.; Yin, X.; Ning, J. Trustworthy Announcement Dissemination Scheme with Blockchain-Assisted Vehicular Cloud. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 1786–1800. [CrossRef]
19. Moll, P.; Patil, V.; Zhang, L.; Pesavento, D. Resilient Brokerless Publish-Subscribe over NDN. In Proceedings of the MILCOM 2021–2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November–2 December 2021; pp. 438–444.
20. Bidóia, M.C.; Cavenaghi, M.A.; Spolon, R.; Spolon, R.; Manacero, A., Jr.; Lobato, D.C. Simulation of a centralized reputation system for vanets. In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA), Las Vegas, NV, USA, 21–24 July 2014; p. 1.
21. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
22. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **2017**, *13*, 184–195.
23. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
24. Javed, M.U.; Rehman, M.; Javaid, N.; Aldegheishem, A.; Alrajeh, N.; Tahir, M. Blockchain-based secure data storage for distributed vehicular networks. *Appl. Sci.* **2020**, *10*, 2011. [CrossRef]
25. Li, M.; Weng, J.; Yang, A.; Liu, J.N.; Lin, X. Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11248–11259. [CrossRef]
26. Li, S.; Wang, X. Quickest attack detection in multi-agent reputation systems. *IEEE J. Sel. Top. Signal Process.* **2014**, *8*, 653–666. [CrossRef]
27. Zhang, Z.; Yu, Y.; Zhang, H.; Newberry, E.; Mastorakis, S.; Li, Y.; Afanasyev, A.; Zhang, L. An overview of security support in named data networking. *IEEE Commun. Mag.* **2018**, *56*, 62–68. [CrossRef]
28. Kumar, N.; Singh, A.K.; Aleem, A.; Srivastava, S. Security attacks in named data networking: A review and research directions. *J. Comput. Sci. Technol.* **2019**, *34*, 1319–1350. [CrossRef]
29. Suksomboon, K.; Tarnoi, S.; Ji, Y.; Koibuchi, M.; Fukuda, K.; Abe, S.; Motonori, N.; Aoki, M.; Urushidani, S.; Yamada, S. PopCache: Cache more or less based on content popularity for information-centric networking. In Proceedings of the 38th Annual IEEE Conference on Local Computer Networks, Sydney, NSW, Australia, 21–24 October 2013; pp. 236–243.
30. Yao, L.; Wang, Y.; Xia, Q.; Xu, R. Popularity prediction caching using hidden markov model for vehicular content centric networks. In Proceedings of the 2019 20th IEEE International Conference on Mobile Data Management (MDM), Hong Kong, China, 10–13 June 2019; pp. 533–538.
31. Yao, L.; Wang, Y.; Wang, X.; Guowei, W. Cooperative caching in vehicular content centric network based on social attributes and mobility. *IEEE Trans. Mob. Comput.* **2019**, *20*, 391–402. [CrossRef]
32. Ullah, S.S.; Ullah, I.; Khattak, H.; Khan, M.A.; Adnan, M.; Hussain, S.; Amin, N.U.; Khattak, M.A.K. A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things. *IEEE Access* **2020**, *8*, 98910–98928. [CrossRef]
33. Sabir, Z.; Amine, A. BIoVN: A Novel Blockchain-Based System for Securing Internet of Vehicles Over NDN Using Bioinspired HoneyGuide. In *Advances in Blockchain Technology for Cyber Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 177–192.
34. Naeem, M.A.; Nguyen, T.N.; Ali, R.; Cengiz, K.; Meng, Y.; Khurshaid, T. Hybrid cache management in IoT-based named data networking. *IEEE Internet Things J.* **2021**, *9*, 7140–7150. [CrossRef]
35. Khelifi, H.; Luo, S.; Nour, B.; Moungla, H.; Ahmed, S.H. Reputation-based blockchain for secure NDN caching in vehicular networks. In Proceedings of the 2018 IEEE Conference on Standards for Communications and Networking (CSCN), Paris, France, 29–31 October 2018; pp. 1–6.
36. Kim, D.; Nam, S.; Bi, J.; Yeom, I. Efficient content verification in named data networking. In Proceedings of the 2nd ACM Conference on Information-Centric Networking, San Francisco, CA, USA, 30 September–2 October 2015; pp. 109–116.
37. Chen, C.; Wang, C.; Qiu, T.; Lv, N.; Pei, Q. A secure content sharing scheme based on blockchain in vehicular named data networks. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3278–3289. [CrossRef]
38. Lei, K.; Zhang, Q.; Lou, J.; Bai, B.; Xu, K. Securing ICN-based UAV ad hoc networks with blockchain. *IEEE Commun. Mag.* **2019**, *57*, 26–32. [CrossRef]
39. Bernardini, C.; Silverston, T.; Festor, O. MPC: Popularity-based caching strategy for content centric networks. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 3619–3623.
40. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J. A reputation-based announcement scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
41. Hussain, S.; Ullah, S.S.; Ali, I. An efficient content source verification scheme for multi-receiver in NDN-based Internet of Things. *Clust. Comput.* **2022**, *25*, 1749–1764. [CrossRef]

42. Karunathilake, T.; Förster, A. A Survey on Mobile Road Side Units in VANETs. *Vehicles* **2022**, *4*, 482–500. [CrossRef]
43. Ren, Z.; Zhang, F.; Zheng, G.; Saleem, A.; Guan, K. A 3D non-stationary channel model with moving mobile station in rectangular tunnel. *Int. J. Antennas Propag.* **2019**, *2019*, 6750153. [CrossRef]