Reputation-based Blockchain for Secure NDN Caching in Vehicular Networks

Hakima Khelifi*, Senlin Luo*, Boubakr Nour‡, Hassine Moungla§¶, and Syed Hassan Ahmed‖
*School of Information and Electronics, Beijing Institute of Technology, Beijing, China
‡School of Computer Science, Beijing Institute of Technology, Beijing, China
§LIPADE, University of Paris Descartes, Sorbonne Paris Cite, Paris, France
¶UMR 5157, CNRS, Institute Mines Telecom, Telecom SudParis, Nano-Innov CEA Saclay, France
‖Department of Computer Science, Georgia Southern University, Statesboro, GA 30460, USA
Emails: {hakima,luosenlin,n.boubakr}@bit.edu.cn, hassine.moungla@parisdescartes.fr, sh.ahmed@ieee.org

Abstract—**Enormous research efforts have been investigated in Vehicular Ad Hoc Networking to improve users safety, traffic condition, and provide different reliable services, that are challenging tasks to accomplish in the current Internet model. In-network caching is one of the promising features of Named Data Networking, a new future Internet architecture based on content name instead of the host address. It aims to enhance the network performance, data availability, distribution, and access. The applicability of NDN in VANET introduced several issues, especially in the security and trust relationships. In this paper, we present a reputation-based blockchain mechanism to secure the cache in the vehicular environment and enhance the trust between cache stores and consumer vehicles. The obtained results demonstrate that our scheme outperforms the normal NDN behavior by providing only trust content in the network.**

I. INTRODUCTION

In the last decades, there has been a growing interest in Vehicular Ad-hoc Networks (VANETs) [1] from both industry and academia sectors, where various solutions have been proposed to improve driving safety, and manage traffic conditions. Vehicles are the main elements in VANET networks, they exchange a huge amount of information with other vehicles (V2V) or infrastructures (V2I). Different challenges faced the realization of vehicular environments including the high dynamic topology caused by the frequently links connection and disconnection with a very short time, and the high mobility of vehicles [2]. Moreover, VANET is an unbound network that affects negatively in the definition of standardization and security rules and policies. These properties made the delivery data hard and challenged task under IP-based networking solutions.

On the other hand, and due to the change in users' and applications' requirement, the Internet is shifting away from the connectivity toward the content-oriented paradigm. Information-Centric Networking [3] has been proposed as a new future Internet architecture that uses the content name as the main element to exchange data instead of using host devices [4]. By decoupling the content from its original location, all security mechanisms are applied to the content itself rather than the communication channel. Hereby, the in-network caching can be applied, where any node may cache and serve the content. Under the concept of ICN, various architectures have been implemented. Name Data Networking [5] is one of the most promising ICN architecture that uses names in the process of routing and forwarding data. NDN implements an Interest-Data exchange model, with content-based security by embedding all security-related information in the data packet. Also, NDN in-network caching feature is promising to enhance the content distribution in the network, improve the data access by reducing the delay [6].

Most of existing NDN efforts targeting VANET [7], [8] are basically on routing and forwarding aspects [9], [10]. However, the security aspect [11] and especially secure in-network caching is not well investigated, and has less attraction by researchers. In-network caching may get affected in different scenarios, from different network levels, under numerous attacks such as Denial of Service (DoS) attack, Wormhole Attack, Bogus Information attack, Replay Attack, and Timing Attack [12]. Since NDN allows nodes to cache any received data without any rules or policies, attackers get more chance to easily aggressive the content store, malicious nodes may serve a poisoned content in the network, they can pollute the cache store and isolated users from the corrected and valid content.

In order to solve the aforementioned issues, and overcome the missing trust among cache stores and data consumers, we proposed in this paper a reputation-based blockchain to secure NDN cache content in a vehicular environment. The proposed solution aims to cache only the trust content in intermediate node cache store, consumers may ask for content and consume only valid, hereby they evaluate the reputation of the served cache store by increasing its reputation on a blockchain network. The use of blockchain is motivated by its solid architecture for any modifications and the use of proof-of-work.

The rest of the paper is organized as follows: in the next section, we overview the blockchain technology, and review some of the existing solutions on NDN-based VANET. After, we present our solution in section III, we discuss the system architecture and network elements, the creation of blocks and the different process from data request, to caching, until consuming and evaluation the cache stores. Then, we discuss the evaluation of the solution is section IV, and conclude the

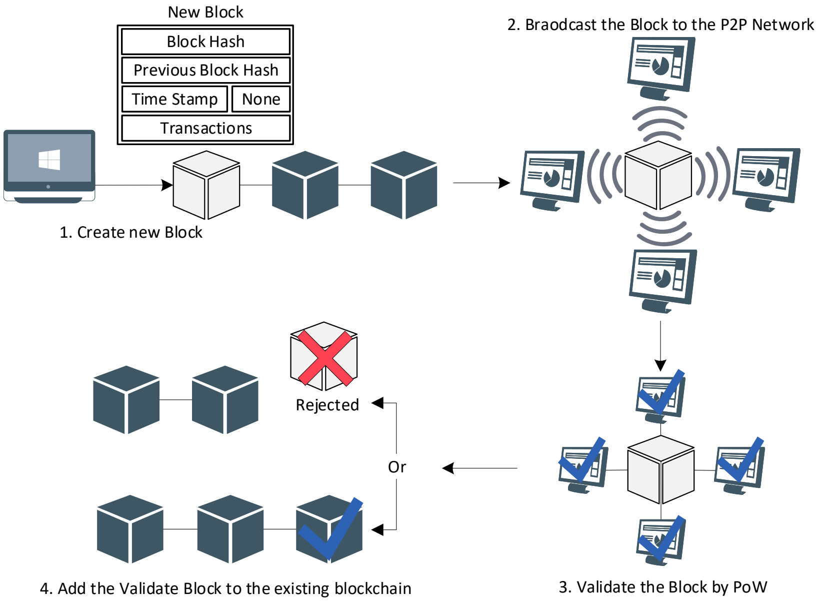
New Block
Block Hash
Previous Block Hash
Time Stamp
None
Transactions
1. Create new Block
2. Braodcast the Block to the P2P Network
3. Validate the Block by PoW
Rejected
Or
4. Add the Validate Block to the existing blockchain

Fig. 1. Blockchain Example

paper in section V.

II. Background & Related Works

This section provides an overview on blockchain technology, and a state-of-art on NDN Security and Trust over vehicular networks.

A. Blockchain Overview

A few recent years, Blockchain [13] attracted many researchers in different domains, it has been developed to perform the digital cryptocurrency Bitcoin [14], and now it runs as support of distributed peers, providing services to several applications like banking, healthcare, supply chain and Internet of Things.

The Blockchain is a collection of blocks that contain information, this information is open to anyone but is almost impossible to change it. Technically, the first block in the chain is named genesis block, and has not any parent block. Each block includes data, the hash of the block and the hash of the previous block. Usually, the data is depending on the type of blockchain applications, for example, the Bitcoin saves the details of the transaction between nodes and their amount of coins. The hash part is as a fingerprint of the block and is always unique, where if the inside of the block changed, the hash of block would change which make all subsequent blocks invalid. This technique makes blockchain extremely secure. However, the use of hash techniques is not enough to detect the changing of blocks because of the existing of fast computer today that can calculate and measure hundreds of thousands of hashes per instant. That caused an easy changing in the block and then recalculate all of the hashes of rest of the blocks which make the changed blockchain valid.

To overcome this issue, blockchain used the called proof-of-work (PoW) [15] that slows down the creation of each new block. For example, in Bitcoins, the creation of new block took few minutes from the calculation of its PoW and joined to the chain, for that change in one block need to recalculate all following blocks and their PoW, that make it an extremely hard task. Accordingly, the security of blockchain is based on its creation that used hashing and the PoW mechanisms.

As blockchain utilize the peer-to-peer network, anyone can easily be joined and get the same capacity of information about the blockchain. An example of blockchain architecture and its work illustrated in Figure 1. When the node creates a new block, it sends this block to other nodes. Other "mining" nodes collect block information and try to make it valid, where they perform their PoW by repeatedly modifying the nonce values of the blocks till the hash complete. Then the node that creates this block broadcasted in the network, and every node examined the PoW of the block and accepted if it is valid. After checking the block, each node adds and stores this new block to its blockchain.

Blockchain Efforts in VANETs: Several works took the advantages of blockchain and merged it in vehicular networks, such as the intelligent vehicle [16], V2X communications [17], and smart city [18]. However, and to the authors' best knowledge, our work is the first that brings blockchain to NDN-based vehicular networks. This paper proposes a new secure reputation-based NDN cache based on blockchain for vehicular communication.

B. Security and Trust in NDN-based Vehicular Networks

NDN is a receiver-driven architecture that replaces the IP addresses by hierarchical names. NDN uses the content name as the main network element along with Interest and Data packets to forward and deliver content. Nodes in NDN maintained three data structures: *Content Store* (CS) that is

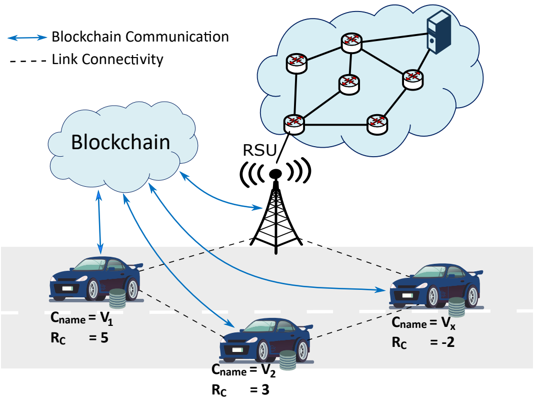

Fig. 2. System Components

used to cache the content, *Pending Interest Table* (PIT) to keep trace of Interests and used to deliver data back to requesters, and *Forwarding Information Base* (FIB) as the routing table.

NDN is promising to change the way the Internet work, toward this, researchers showed their efforts to bringing NDN to the vehicular network [19] tending to create enhance the scalability, reliability, and provide a securable network. However, VANET security requirements are still challenging to fulfill due to the high dynamic topology, unbounded networks, sensitive time and dissemination content [20]. From the other hand, NDN still has various security and privacy issues [21] including naming, signature, and caching privacy, which make the merger more challenging.

Assuming an example where a vehicle requests a content by specifying its name, the Interest packet will be passively broadcasted to all neighbors, hereby they will create a PIT entry and forward the requests upstream if no data found in the cache store. A malicious node may create a fake data packet and send it to the requester, that will expunge PIT entry from intermediate nodes. The content is not valid, and the consumer will never get the valid content version as the fake reply expunge PIT entry. Similarly, any intermediate node may reply with fake data, acting as it is the valid one from its own cache store. Malicious node acts as a non-trust cache store in the network. Moreover, the attack may go beyond that, where a list of node pollute the trust cache store by making a storm of requests and changing the cached content distribution, a non-valid non-popular content will be cached and may be served. The trust of cache store, cache poisoning, and cache pollution attacks are very critical in NDN network.

Some solutions have been designed to deal with these attacks, basically in from NDN perspective [22]–[24], where vehicular network have not been taken into consideration. However, these solutions may not work in VANET due to its challenging characteristics. Thus, the main motivation of this work is to propose a solution that should secure the vehicular network, overcome the insecure cache store, and enhance the trust among replica nodes and consumers.

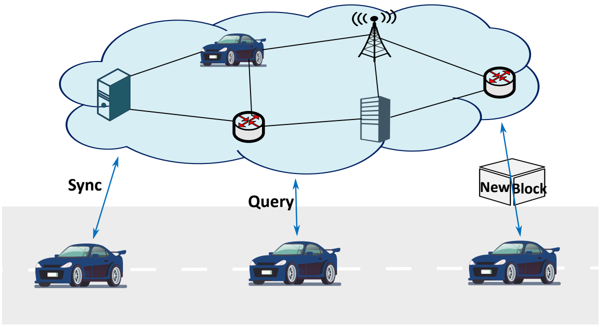

Fig. 3. Blockchain Architecture

III. PROPOSED BLOCKCHAIN-BASED MECHANISM

In-network caching is one of the most important features in ICN/NDN, it aims to enhance the data access and reduce communication delay. However, and due to the fact that any node may cache and serve the data, trust and data security is a very paramount issue. In the following, we present our blockchain-based solution to secure the caching and enhance trust relationship.

A. System Component

In a vehicular environment, vehicles can act as data consumers/producers, the requested data may be served by Cloud or Internet-based applications, most of the requests are routed/forwarded through a Road Side Unit (RSU). By bringing NDN to VANET, vehicles can play the role of replica nodes where they have the ability to cache the data and serve it for future requests. Similarly, RSUs and any intermediate node can cache the content. This uncontrolled and administrative-less cache possibility leads to the case of untrusted cache store in the network.

Thus, we assign to each cache store a name C_{name}, and a reputation-value R_c. Initially, the system assigns to any newly connected node a reputation-value to indicates the degree of its reputation as a cache store. This value is kept updated based on the data that the node served from its cache store. The highest value, the more trust the node is. Figure 2 depicts the different technologies and components used in the system.

B. Blockchain Architecture

In this paper, we integrate blockchain as a decentralized/distributed trust platform on top of NDN-based VANET. Thus, our proposed mechanism has mainly two basics technologies including communication network enabled NDN devices, and blockchain technology. Furthermore, and as vehicles/RSUs have no limitations in processing and storage, they can act as blockchain *miner* nodes by implementing the proof-of-work, validating, broadcasting, and storing the transactions in the network. Similarly, data consumers and providers act as *listeners* by adding the new valid blocks to the blockchain. Figure 3 illustrates the proposed blockchain architecture.

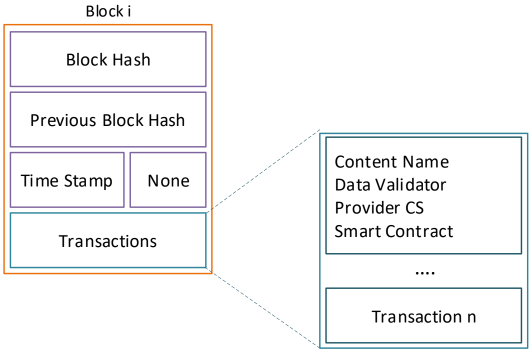

Fig. 4. Structure of Block

1) Structure of Block: Our reputation-based mechanism aims to assign each intermediate node an initial *reputation-value*, this value will be increased by time only if the cache store served a trusted content. After verifying of the content is valid or not by the content consumer, it sends an update to the blockchain network informing about the served cache store either by increasing to decreasing its reputation value.

A general block structure is illustrated in Figure 4, that has the following fields:

- *Data Validator*: fundamentally, the *Data Validator* is the same content requester, and it serves to validate if the content served by the CS is valid or not. Then, it updates CS's reputation-value R_c in the blockchain network.
- *Provider CS*: is the intermediate node who served the request issued by the *Data Validator*, and whose will get a new reputation-value.
- *Content Name*: is the name of the content requested by the *Data Validator* and served by *Provider CS*.

The reason of adding *Content Name* in the block structure is to keep tracking the different content traversed the network, not only the cache stores, and finding out the valid content with the valid name, hereby we drastically enhance the data/user privacy, by enforcing content copyright, and solving the issue of sharing the same content/data using the different name.

2) Naming Convention: NDN provides hierarchical names to identify both root-prefix and content. Application designers have the ability to propose names based on their needs and application level semantics. Thus, we propose, and without violating NDN naming design, a three-level hierarchical name structure, as shown in Figure 5.

- *Root Prefix*: defines the core network prefix or the application name.

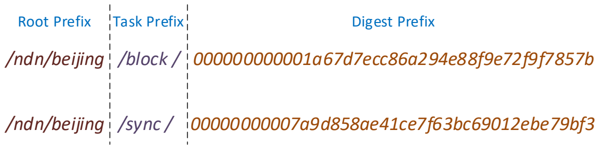
Root Prefix
Task Prefix
Digest Prefix
/ndn/beijing
/block /
000000000001a67d7ecc86a294e88f9e72f9f7857b
/ndn/beijing
/sync /
00000000007a9d858ae41ce7f63bc69012ebe79bf3

Fig. 5. Hierarchical Naming Convention

Algorithm 1: Upstream Forwarding Process

```
Input: $N$: Requested Content Name
if ($N$ in CS) then
    D := Generate Data packet;
    Add $C_{name}$ to Data packet;
    Send Data packet to the same received face;
else
    if ($N$ in PIT) then
        Add received face to PIT entry;
        Drop Interest packet;
    else
        if ($N$ in FIB) then
            Find next-hop;
            Forward Interest packet;
        else
            Drop Interest packet;
        end
    end
end
```

- *Task Prefix*: identifies and classifies the information exchange method into two main classes; either *Block* (e.g., getting/adding the block) or *Sync* to synchronize block between peers.
- *Digest Prefix*: identifies the message digest of the previous block hash. This prefix is used to show the position of the current block in the chain.

C. Content Caching & Forwarding

Typically, the Cache Store (CS) is involved only in the Interest forwarding, in order to find a match and serve the data rather than forwarding the Interest upstream. While during the data forwarding, the CS is consulted only if the data packet needs to be cached according to the deployed local caching strategy.

In addition to content name in the data packet, here we propose to add the name of the cache store (intermediate node) in the data packet that helps the consumer node to identify *Provider CS* and add it in the block. Algorithm 1 shows the Interest Forwarding process. When an intermediate node receives a data packet, after performing PIT lookup, the data will be cached according to the cache policies, here we propose that NDN engine queries blockchain asking about the provider CS's reputation. The cache will only be applied if the node has a good reputation regardless of the deployed caching strategy.

It is noteworthy to highlight that the Algorithm 2 is not a new caching scheme. However, it is a verification routine that should be executed posterior the caching scheme decision.

D. Data Consuming

After the consumer receives that data, it first checks the reputation of the served cache store. This verification can be done by consulting the blockchain network for content and

Algorithm 2: Caching policy

```
Input: N: Requested Content Name
if (Caching Policy allows Data Cache) then
    Query BC about $R_C$;
    if ($R_C$ > Threshold) then
        Cache the data;
    else
        Skip cache;
    end
```

CS names. According to the defined rule in the network, the consumer may/may not consume the content if the reputation did not reach some threshold. Also it can re-issue the same Interest asking for other replies. Algorithm 3 shows the content consuming routine, and explained as follows:

New Block Creation: After consuming/validating the received data, the consumer will explicitly create new block informing the blockchain network about its validation, including the content name, the served CS name.

Updating Status: The PoW enforces that only the legitime blocks can be added to the blockchain, all new blocks must be validated by the network peers before chaining them.

IV. EVALUATION & DISCUSSION

In order to show the efficiency of our proposed solution, we have used a scale-free network topology that based on Barabasi-Albert model [25]. Then we have calculated the number of contents valid/trust in the network versus the non-valid data that have been created by malicious nodes and might be cached by replica-nodes or consumed by vehicles.

Furthermore, as the proposed solution can be run on top of different caching schemes, we used three different caching placement strategies including Leave Copy Everywhere (LCE), Leave Copy Down (LCD), and Edge Caching [26]. In LCE, all nodes in the delivery path cache the content, while in LCD only nodes after the producer are selected as cache replica, in the downstream. EC also selects nodes that are in consumers' edge.

Algorithm 3: Content consuming routine

```
Input: D: Data Packet
Query BC about $R_C$ of $C_{name}$;
if ($R_C$ > Threshold) then
    Consuming Data;
    Create new block;
    if (D is Valid) then
        $R_C$ ++;
    else
        $R_C$ --;
    end
    Broadcast the Block;
else
    Discard Data packet;
    Re-issue Interest;
end
```

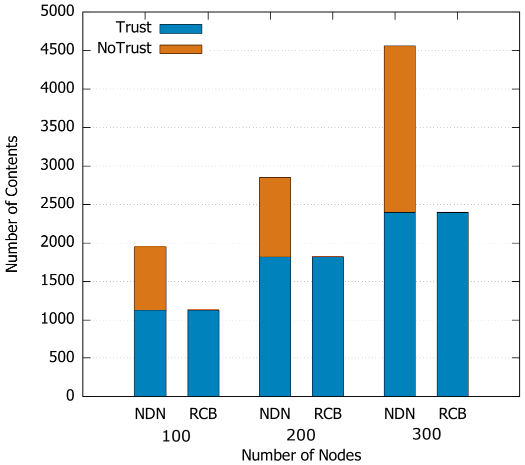

Fig. 6. Number of trust and non trust contents in CS per node

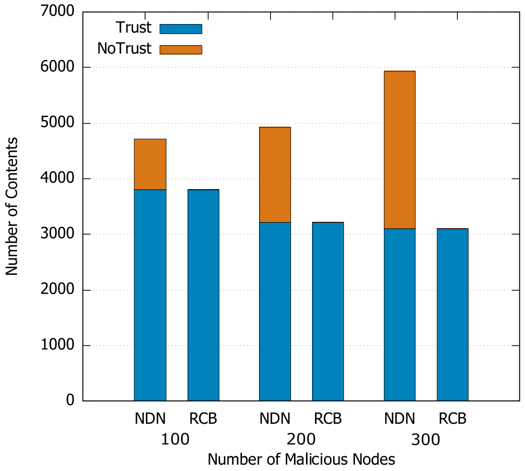

Fig. 7. Number of trust and non trust contents in CS per malicious node

Consider Figures 6 and 7, which plot the number of cached content in network versus the number of overall nodes and the number of malicious nodes respectively. NDN's normal behavior caches all content regardless of its validation (blind caching), thus we can see that the number of cached content keeps increasing with a near-equality between trust and non-trust content, whereas by using the reputation-based mechanism, only the trust content are cached in cache stores, and served by intermediate nodes, with a zero non-trust content in the cache stores.

It is important to highlight here that we are measuring only the trust in the network, it is clear that serving only trust/valid content from the cache store with radically enhance network performance by avoiding re-requests from consumers, and drastically creates a secure system.

Figure 7 proves that by showing whether the number of malicious nodes increases, the proposed solution caches only the valid content. Based on the deployed placement scheme,

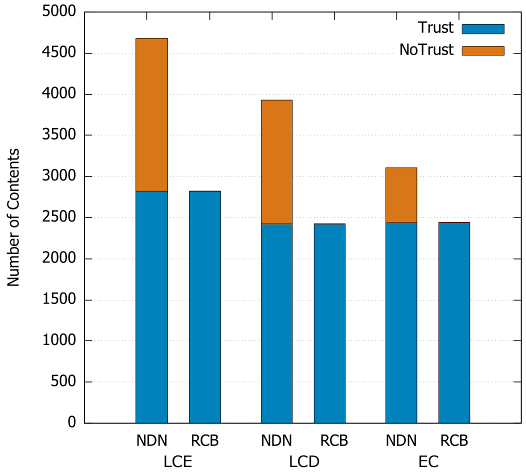

Fig. 8. Number of trust and non trust contents in CS with different caching schemes

the amount of cached content differ, as well as the number of non-trust content. Such cases are well-seen in Figure 8, LCE caches all content among the forwarding path, while LCD and EC only one-hop after producer or consumers respectively, and because producers may have different neighbors in compared to consumers that are attached to only one edge/gateway node, LCD caches more content than EC.

V. CONCLUSION

The distributed NDN in-network caching contributes to enhance the network performance, data availability, and content access. However, the involvement of non-trust nodes in the process may create various security and privacy issues. In this paper, we proposed a reputation-based blockchain scheme to enforce the trust between consumers and cache stores, and secure the caching in a vehicular environment. The proposed scheme is based on blockchain network, and consists of assigning each cache store a reputation value, that gets increase/decrease based on the served content. The proposed solution is totally independent from the deployment cache placement policy and can be run on top of any caching scheme. The results show that only the secure content shall be cached and served in the network. The next stage of our research will be the deployment of the proposed scheme on real NDN testbed and merge with cross-industry blockchain technologies such as Hyperledger.

ACKNOWLEDGEMENTS

The work of S. Luo was supported by the National 242 Project under Grant No. 2017A149. Dr. Luo is the corresponding author.

REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[2] M. Laroui, A. Sellami, B. Nour, H. Moungla, H. Afifi, and S. Boukli-Hacéne, "Driving Path Stability in VANETs," in *IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[3] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, 2012.

[4] B. Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu, "M2HAV: A Standardized ICN Naming Scheme for Wireless Devices in Internet of Things," in *International Conference Wireless Algorithms, Systems, and Applications*, 2017.

[5] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos *et al.*, "Named Data Networking (NDN) Project," *Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC*, 2010.

[6] B. Nour, K. Sharif, F. Li, H. Moungla, A. E. Kamal, and H. Afifi, "NCP: A Near ICNCache Placement Scheme for IoT-based Traffic Class," in *IEEE Global Communications Conference*, 2018, pp. 1–6.

[7] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: A content-centric framework," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60–66, 2017.

[8] H. Khelifi, S. Luo, B. Nour, A. Sellami, H. Moungla, and F. Naït-Abdesselam, "An Optimized Proactive Caching Scheme based on Mobility Prediction for Vehicular Networks," in *IEEE Global Communications Conference*, 2018, pp. 1–6.

[9] G. Mauri, M. Gerla, F. Bruno, M. Cesana, and G. Verticale, "Optimal content prefetching in NDN vehicle-to-infrastructure scenario," *IEEE Transactions on Vehicular Technology*, pp. 2513–2525, 2017.

[10] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 873–876, 2017.

[11] H. Khelifi, S. Luo, B. Nour, and S. C. Shah, "Security & Privacy Issues in Vehicular Named Data Networks: An Overview," *Mobile Information Systems*, 2018.

[12] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[13] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *IEEE International Congress on Big Data*, 2017, pp. 557–564.

[16] M. Singh and S. Kim, "Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain," *arXiv preprint arXiv:1707.07442*, 2017.

[17] R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, and F. Kargl, "Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication," *arXiv preprint arXiv:1710.08891*, 2017.

[18] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart City," *Journal of Information Processing Systems*, vol. 13, no. 1, p. 84, 2017.

[19] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: a survey and future perspectives," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 98–104, 2016.

[20] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications*, 2017.

[21] T. Chatterjee, S. Ruj, and S. D. Bit, "Security Issues in Named Data Networks," *Computer*, vol. 51, no. 1, pp. 66–75, 2018.

[22] D. Kim, J. Bi, A. V. Vasilakos, and I. Yeom, "Security of Cached Content in NDN," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2933–2944, 2017.

[23] M. Conti, P. Gasti, and M. Teoli, "A lightweight mechanism for detection of cache pollution attacks in named data networking," *Computer Networks*, vol. 57, no. 16, pp. 3178–3191, 2013.

[24] S. DiBenedetto and C. Papadopoulos, "Mitigating poisoned content with forwarding strategy," in *IEEE Conference on Computer Communications Workshops*, 2016, pp. 164–169.

[25] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[26] I. U. Din, S. Hassan, M. K. Khan, M. Guizani, O. Ghazali, and A. Habbal, "Caching in Information-Centric Networking: Strategies, Challenges, and Future Research Directions," *IEEE Communications Surveys & Tutorials*, 2017.