BIoVN: A Novel Blockchain-Based System for Securing Internet of Vehicles Over NDN Using Bioinspired HoneyGuide

Zakaria Sabir and Aouatif Amine

1 Introduction

Researchers and manufacturers discuss and develop ITS to achieve road safety and comfortable driving (intelligent transportation systems). Current vehicles already have a set of modern technologies deployed. For instance, they can run various applications, use navigation systems, and connect to the Internet. The following purpose is achieving V2V (vehicle-to-vehicle) [1] and V2I (vehicle-to-infrastructure) [2] communications to enhance safety messages exchanged between road users [3].

Vehicular networks are characterized by dynamic topology and high connectivity, which is an issue for the current Internet architecture based on the TCP/IP model. Therefore, research communities proposed to bring NDN (named data networking) to IoV (Internet of vehicles) to tackle those issues. NDN is a future Internet architecture that is based on named content rather than IP addresses. It uses a request/reply model which doesn't need session establishment nor address allocation to exchange data.

In terms of security, NDN came with a new model that uses public and private keys to encrypt and decrypt data in the network. The main idea is to secure the data itself rather than securing the medium of transmission. However, additional security concerns still exist in NDN and require further research [4]. Thus, we thought to bring the blockchain technology to NDN-based IoV, especially to overcome the cache poisoning attack that intends to propagate bogus content to the network's nodes, and thereby to forward only safe content. Blockchain is a decentralized, distributed, and open ledger that saves transactions efficiently in a transparent and immutable way.

Z. Sabir (✉) · A. Amine
Ibn Tofail University, ENSA, Kenitra, Morocco
e-mail: za-karia.sabir@uit.ac.ma; aouatif.amine@uit.ac.ma

Y. Maleh et al. (eds.), *Advances in Blockchain Technology for Cyber Physical Systems*, Internet of Things, https://doi.org/10.1007/978-3-030-93646-4_8

This paper proposes a novel blockchain-based system for securing IoV over NDN, called BIoVN (**b**lockchain for **I**nternet **o**f **v**ehicles over **N**DN). The proposed system aims to deliver, forward, and cache only safe content over the network. To the best of our knowledge, very few publications are available in the literature that discusses the IoV over NDN in terms of blockchain technology or addresses the security of the cached and forwarded content.

We also propose a new bioinspired algorithm of HG (HoneyGuide), which we used in the BIoVN system. The principal aim of any algorithm is to discover the most outstanding couple between a collection of possible results and a goal model. This can be approached to discovering a fulfilling result in discrete search space over a reasonable execution time. Representing the problem in this manner makes it very much similar to the attitude of an optimization algorithm. Indeed, metaheuristics are considered repetitive actions that cleverly lead a subordinate heuristic to create excellent results by operating diversification and intensification methods in the space. Metaheuristics are approximate algorithms that exceed exact algorithms regarding the scope of the resolved problem. The capacity to deal with different difficulties using miniature variations usually comes from the nature inspiration. Using easy tools, different problems are resolved in nature, and a quality result is always found thanks to the attitude of living beings such as animals and insects. Therefore, we tried to discover an effective metaheuristic stimulated by the power of nature to resolve complicated problems and produce results with acceptable quality. Currently, we are in the phase of the simulation of the system. The major contributions of this work are twofold as follows:

- To prevent malicious vehicles from broadcasting poisoned content, we designed a novel reasonable blockchain-based security architecture for IoV over NDN, which ranks different nodes in the network and allows only trusted ones to exchange interest and data packets.
- We proposed a new bioinspired algorithm of the name HG, which we used in the BIoVN system.

The remainder of this paper is organized as follows: Sect. 2 presents an overview of NDN and blockchain technologies, Sect. 3 summarizes the related work, and Sect. 4 describes the proposed method. Finally, we conclude the paper.

2 Overview of NDN and Blockchain Technologies

Named Data Networking

NDN (named data networking) is an instance of ICN (information-centric networking) [5], which is recognized as a significant field of study. Among instances of ICN, NDN is proposed as a promising future Internet architecture, and it is based mainly on the content (what to send) instead of the location (where to send). Named data

packets are used rather than destination and source addresses used by the current TCP/IP architecture [6]. While forwarding is done using IP address headers in IP-based routers, each packet name prefix is used by NDN-based routers to forward packets. This adoption of unique named contents allows nodes to memorize and control the state of each packet. NDN and the current Internet architecture have the same hourglass architecture except for some divergence in similar layers [7]. The named content chunks constitute the principal blocks of NDN, while in TCP/IP, the basic unit of communication is a point-to-point channel between two nodes identified by IP addresses [8, 9].

Two types of packets are engaged in NDN: interest and data [10]. They are used, respectively, by consumers and producers while communicating. Since the NDN is recipient driven, consumers express their desire for a piece of data by putting its name in an interest packet and sending it to the network. Any node which retains a copy of the desired content will play the role of the producer and reply with a data packet. This packet will then take the reverse path to come back to the consumer [11]. Each node maintains three databases [12] used in the forwarding process: the CS (Content Store) stores copies of freshly forwarded data to supply future queries and increase content distribution. The PIT (pending interest table) keeps track of forwarded interest packets that are not yet satisfied. Incoming interfaces are saved in the PIT entries, so data packets can easily retrieve the correct path to reach original consumers. And the FIB (forwarding information base) records the important forwarding information like the prefix and the next hopes. This information is used to lead the interest packet to the potential providers.

Figure 1 illustrates an example of NDN-based IoV architecture. In this example, the content "/parking/ Mimosas/P3" is desired by Consumer 1. As the forwarder has this content in its cache, it will send it directly to Consumer 1 without forwarding it to the initial producer. However, the content "/traffic/highway/A5/20" desired by Consumer 3 will be transferred to the initial producer. If Consumer 2 also expresses an interest in the same content, Consumer 3 will aggregate this request in its PIT and not forward it. Once the producer sends the data packet to the forwarder, the latter will forward it to Consumer 3, which will forward it in its turn to Consumer 2 thanks to the PIT entries.

Blockchain Technology

Blockchain technology is a distributed peer-to-peer network and an open ledger that Satoshi Nakamoto first implemented for Bitcoin [13]. In contrast to the traditional centralized ledger systems, all the participants in the network keep together a copy of the distributed ledger with the help of a consensus algorithm. Every user is authorized to add or modify data to solve a complex mathematical puzzle. Every participant in a blockchain system is recognized with a cryptographic public key shared with other users so they can interchange information. The private key, in contrast, is kept stored securely in the client's equipment. In blockchain technology,

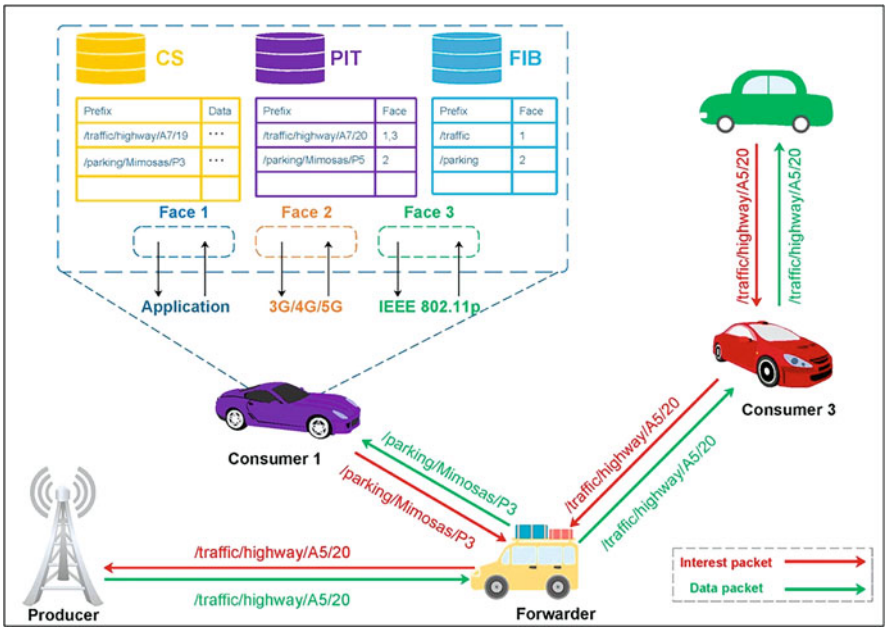

Fig. 1 Example of NDN-based IoV architecture

it is highly impossible to succeed an attack in the network system since a private key cannot be derived from a public key, according to [13] and [14]. The transactions in the blockchain are stored in a verifiable and immutable way.

The data structure of the blocks is designed in a specific way that links each block to the previous block via its unique hash value. Trustworthiness and authenticity in the network are established through a consensus algorithm which is considered an important component of the blockchain system. This process is known as "mining," and nodes that participate are called "miners." Mining is done without engaging any third party or central authority [15]. Some examples of consensus algorithms are PoW (proof of work) which is used in Bitcoin; DPoS (delegated proof of stake), which is used in Ethereum; proof of elapsed time; proof of burn; proof of space; proof of luck; and practical Byzantine fault tolerance.

Although blockchain was initially proposed for the commercial industry, it is currently revolutionizing different fields. It can support diverse applications and services [16] such as IoT (Internet of things), banking system, stock market trading, supply chain management, government record, hospitalization, voting, and property transfers. Figure 2 depicts an example of a transaction in blockchain.

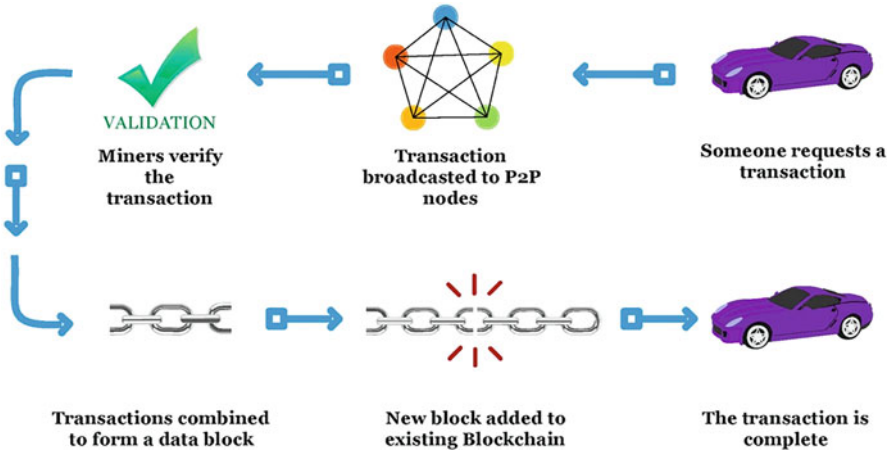

Fig. 2 Example of a transaction in the blockchain network

3 Related Work

Security in NDN-Based IoV

A huge amount of data is being exchanged in vehicular networks. The aim behind these communications is to improve road safety and enhance the driving experience. Securing the exchanged information becomes more important due to the direct impact on human life. Different researchers tried to bring the future Internet architecture NDN to IoV to improve various features, including security.

Authors in [17] proposed IFAMS (Interest Flooding Attack Mitigation Scheme), a new scheme that focuses on mitigating interest flooding attacks in VNDN (vehicular named data networking). They have edited the interest packet to create a new packet field named "consumer_id" which is a unique integer value. They have also assembled the IDs of malevolent vehicles in a table named "restricted id table" maintained by each vehicle. A randomized time value is assigned to every vehicle in the network at the time of ignition. Arsalan et al. [18] proposed a new scheme named TAP (timing attack prevention) to tackle the issue of timing attack in vehicular networks by merging NDN with SDN (software-defined networks). The proposed scheme uses the network controller to mitigate the attacker detected by a legitimate vehicle. To find out the time period in which a packet arrives from the source to the destination, a vehicle first calculates the distance using its coordinates, the sender's coordinates, and the signal propagation speed in the detection process. Then, the time period value is deducted from packet arrival time to get the last vehicle arrival time to check whether the previous vehicle added any delay in the packet or not. Authors in [19] discussed the security of VANET (vehicular ad hoc networks) using a trust function. The trust value of every vehicle interested in receiving data packets

is calculated. They have also calculated the number of occasions an interest packet is shown by vehicles in a forwarding list. Sending data to neighbors is based on the number of vehicles that appear in the route. Manimaran et al. [20] proposed an adaptive IDS (intrusion detection system) for NDN named IDSNDN. Using sensor values present in the vehicle's OBU (on-board unit) and the heartbeat rate value, authors created the rules of the IDS. An additional packet named "sensor packet" is used by the IDS, which is included in the RSUs (roadside units). Once receiving a safety message, the RSU forwards it to the IDS module, verifying it based on the ruleset. If the message turns out to be fake, an alarm is returned.

Blockchain-Based IoV

IoV has become a promising research area recently. By allowing direct information exchange between vehicles, vehicular networks help in reducing traffic congestion. However, malicious vehicles may misguide the whole communication. Blockchain technology is considered a preferred technique to grant security in real-time circumstances to deal with this issue. In [21], the authors proposed a blockchain framework to address the issue of security in intelligent sensors of autonomous and connected vehicles prone to intrusion. The proposed scheme was studied based on different criteria, like a compromise of smart equipment, bogus queries of the user, authentication scenarios, etc. Shrestha et al. [22] presented a public blockchain that stocks the message and node trust in a relevant distributed ledger to solve critical data propagation issues in IoV. Authors created a new type of local blockchain useful for IoV for real-time message dissemination between vehicles up to the borderline of a country. Kudva et al. [23] studied the mitigation of attacks in IoV and proposed a blockchain-based decentralized trust score framework for the engaged vehicles to find block insider attackers. The authors proposed a detection system composed of two levels. In the first one, the trust is calculated individually by nodes, whereas trust scores for nodes are aggregated by a consortium blockchain-based system in the second one. Authors in [24] proposed a blockchain-based secure data sharing system to solve the issue of trust in IoV. This system uses blockchain to store announcement messages. Vehicles that participate either to block generation or to broadcast announcement messages are rewarded by some cryptocurrency. Kang et al. [25] addressed secure sharing and data storage in IoV by exploiting smart contract and consortium blockchain techniques which effectively prevent data distribution without permission. The authors proposed a reputation-based data sharing scheme to grant data distribution between vehicles with high quality.

Bringing blockchain to NDN-based IoV faces a lack of solutions and is still in its early research stage [26, 27]. In this paper [28], different from those studies, the primary purpose is to design a secure and credible NDN-based IoV system. This is the first work that deals with such a system using both a blockchain technology and a bioinspired algorithm to the best of our knowledge.

Bioinspired Algorithms

Metaheuristic algorithms have lately gotten a lot of interest in a variety of domains. The ACOA (ant colony optimization algorithm) [29] is inspired by ant behavior when foraging for food. They use the pheromones to spread the word to the rest of their team after they have located a nice location. A novel modelization approach is included in the BCO (bee colony optimization) [30] to demonstrate bee movement behavior while searching for food sources. For example, in the PSO (particle swarm optimization) [31], a flock of birds searching for grain works together cooperatively and intelligently to explore the surface of the target. The GA (genetic algorithm) is another well-known bioinspired algorithm [32]. Creating a species that can survive in a certain climate is similar to creating a genetic code. In the realm of computer vision, this approach has been used on a regular basis, with great success. The FA (firefly algorithm) is inspired by the firefly insect's behavior of employing light to attract the attention of other fireflies in its vicinity [33]. The BA (bat-inspired technique) [34] is another contemporary optimization algorithm. This method mimics the echolocation feature of bats, which allows them to distinguish between various prey in the shadows. Cuckoo search, according to several studies, outperforms population-based bioinspired algorithms in terms of exploration and is also suitable for large issues [35, 36]. proposes a CS-based optimization approach for extending the life span of a WSN (wireless sensor network). This approach deploys nodes in the network at random and organizes them into clusters once they have been deployed. The CS aids in cutting down on the consumption of energy. There is a proposal in [37] for improving the CS. The authors suggest a solution to the dilemma of the roadside salesperson. When compared to previous methods, the suggested algorithm performed admirably. To address the NDN-based IoV security issue, we devised a novel algorithm we dubbed HG (HoneyGuide) based on the findings from several research domains. It is possible to think of the search for valid vehicles and the detection of fraudulent ones as discrete 2-D explorations in a research area where time doesn't matter. The HG also has the benefit of having a large variety of settings. Unlike other bioinspired algorithms, the HG method only uses two parameters: the likelihood that the owner bird would discover the honeyguide's eggs and the population size (how many caves in the primary population). The suggested technique and the HG algorithm will be discussed in more detail in the next section.

4 Proposed Method

In this section, we first discuss the security of NDN-based IoV and present our proposed algorithm HG (HoneyGuide). Subsequently, we describe our proposed blockchain-based system for securing IoV over NDN.

Security of NDN-Based IoV

Enabling IoV over TCP/IP has always caused various technical issues; thus, research communities started to propose various methods to bring the future Internet architecture NDN to IoV. Since data names are used in this architecture, there is no need to establish sessions or allocate addresses to exchange data, making it a bright solution to enable effective vehicular communications. Applying NDN to IoV is very beneficial in various properties such as in-network caching, mobility and routing, and in-data security. The latter is the primary concern of this work. NDN looks at security as the main component of the data itself; it doesn't rely on the transmission medium anymore. Since all the vehicles in the network have the ability to cache content, the security attributes of the data packets have to be decoupled from their locality.

The producer uses its cryptographic key to sign each data packet by binding the content to its name while creating data. This allows any user of the network to check the integrity of the data packet. Applications in NDN must use data signatures and cannot drop security.

Nevertheless, additional security concerns still exist in NDN and require further research. Basically, two kinds of attacks need more investigation: interest flooding attack aims to send a tremendous number of interest packets to consume network resources and thus block legitimate requests. A cache poisoning attack aims to propagate fake content to the nodes of the network. Our work is considered as a contribution to resisting the last attack. We believe that blockchain can be a big revolution thanks to its decentralized nature; therefore, we propose a system that brings blockchain to NDN-based IoV to enforce security as explained later in this section.

HoneyGuide Search Algorithm

The HG is a new kind of optimization algorithm, influenced by biological principles. Processing includes using the exploring design of different biological organisms, such as insects and sharks, for its own purposes. In another scene, the HG mimics the honeyguide bird's behavior and reproduces in the same manner.

As a brood parasite (laying one egg in another species' nest), the honeyguide bird prefers hole-nesting species. Honeyguide chicks defecate on or even kill the chicks of the owner bird. They do this by sticking needles in their beaks.

There was an extra day added by the honeyguide female to ensure that her kid hatched before the host's. As a result, the honeyguide infant is constantly a step ahead of the pack in terms of development. It searches for caves in the search region to lay its eggs, and it assigns hatching probabilities to each one based on its findings.

The owner bird may be able to identify honeyguide egg generations in the future. The caverns will be replaced with new ones if this happens. New caverns are

generated at random. We also feel that the area is a search area, with each cave acting as a potential vantage point from which the missing vehicle may be located.

The idea for the suggested technique came from the need to develop a robust vehicular communication algorithm that can function in a variety of challenging situations and with no prior knowledge. The HG method is convenient due to its small number of parameters. It just takes a tiny population to achieve great things. As a result, it is faster than other algorithms since its time complexity is O(n). The "HoneyGuide Search" algorithm is summarized in Algorithm 1.

To begin, the HG algorithm picks a random starting population of "n" subterranean caves at random. There is a fitness function that measures the value of these caves and ranks them according to that value. The cave with the best fitness function also doubles as a better place for eggs to hatch. As a result, there is a good chance it will be a better cave than average. After that, we will use the HG algorithm to determine the quality of the eggs in order to separate out harmful ones from the good ones and keep the good ones safe.

Algorithm 1 HoneyGuide Search

1: Objective function $f(x), x = (x_1, , x_d)$;
2: Generate an initial population of n caves $x_i (i = 1, 2, , n)$;
3: Generate an initial population of m BirdB; $y_j (j = 1, 2, , m)$;
4: Initialize the initial population of BirdB with ranks (RankB);
5: Set MaxIteration;
6: Set RankHB;
7: $Iteration. \leftarrow 0$
8: $j \leftarrow 0$
9: **while** ((j < MaxIteration) or (Stop Criterion)) **do**
10: Evaluate its quality/fitness F_i;
11: **if** $f_i > f_j$ **then**
12: Replace j by the new solution;
13: $RankHB \leftarrow 4$
14: **else**
15: $RankB\, y_j \leftarrow -1$
16: **end if**
17: Iteration ++;
18: j ++;
19: **end while**
20: Post-process results and visualization;

Each cave (search zone) contains a number of eggs that represent vehicles in our case, as shown in Fig. 3. The HG algorithm aims to increase the rank of the HB (honeyguide baby) egg and decrease the rank of the other eggs, after a number of iterations, while this number is lower than the maximum iteration or fixed, the criterion is stopped. To increase the rank of HB (i.e., legitimate vehicle), we have to verify the trustworthiness (see Section "A Blockchain system for securing Internet of Vehicles (BIoVN)"), which is indicated by a fitness function in our case; if the

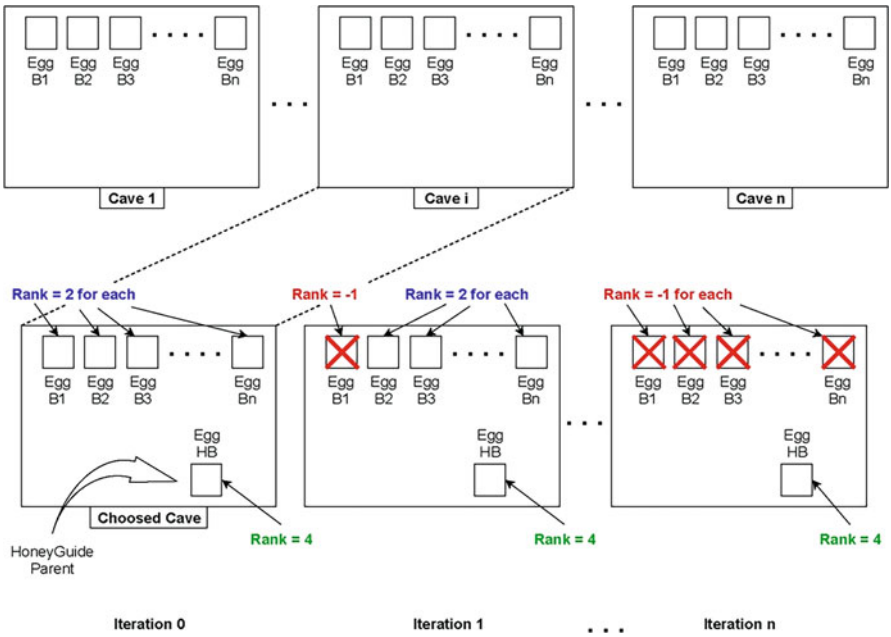

Fig. 3 HoneyGuide search algorithm

fitness function does not satisfy a fixed condition, then the rank of the other eggs (i.e., malicious vehicles) is decreased; so forth, we finally increase the overall quality of the population.

A Blockchain System for Securing Internet of Vehicles (BIoVN)

We believe that blockchain can be a big revolution thanks to its decentralized nature. Therefore, we propose a system that brings blockchain to NDN-based IoV to enforce security. The reasons behind this are summarized in three points:

- In the IoV over NDN, delivering safe content is very important, and blockchain can support this subject as it gives users of the network a new means to keep persistent and accurate databases in a decentralized way and without engaging any other authority.
- Our system belongs to the approaches whereby a rank is calculated and disseminated over a network. Such approaches can reinforce and enhance NDN-based IoV trustworthiness and security by working complementary to the existing systems.
- The design of NDN uses public and private keys to encrypt and decrypt any data in the network, which is homogeneous with the blockchain concept.

System Design

In NDN-based IoV, data privacy and security are crucial obligations. Any vehicle is allowed to cache data packets in its CS to fulfill future interest packets. To prevent malicious vehicles from broadcasting poisoned content, we describe in this part the design of our proposed blockchain-based architecture. As we mentioned before, our system belongs to approaches that calculate ranks for network nodes represented by vehicles in this case. The calculated ranks will be displayed in the blockchain network as transactions.

On the one hand, vehicles and RSUs can play different roles, from consumers to data mules to producers, and they can cache data in their cache stores. On the other hand, malicious vehicles serve their poisoned content and induce caching fake data in the network. For this reason, we suggest assigning a rank "R" to each node in the network; this rank represents the level of trust of the node and has an initial value that can increase or decrease based on the provided content by this node. A reliable content will result in raising the rank of the vehicle and, accordingly, the trust level. A fake content will result in reducing the rank of the vehicle and, accordingly, the trust level. We also propose to create a new table of name MVT (Malicious Vehicles Table), which contains the IDs of malicious vehicles detected over the network. Every node will maintain this table. System architecture

As we mentioned before, our system uses both blockchain and NDN technologies over IoV. Vehicles have different roles (i.e., consumers, data mules, or producers). Meanwhile, they can also be miners when validating transactions and running the consensus algorithm or users when generating transactions and receiving blocks. Vehicular networks are privileged from other ad hoc networks by having unlimited processing and storage capabilities; thus, we assume that vehicles don't have any difficulty dealing with transactions. Figure 4 shows the design of the blocks in the system.

The underlying characteristic of this architecture is the requirement of the peers to discover whether the intention of other nodes in the network is malevolent or honest. The purpose is to allow only legitimate vehicles to accumulate a good trust level. In this manner, non-malevolent vehicles can identify malicious ones easily and eliminate them from the transactions accordingly.

The main transaction exchanged in the BIoVN system is the one that assigns a rank (i.e., trust level) to each vehicle. Once connected to the network, the vehicle receives an initial rank value "R" which is refreshed based on its served content. The rank value raises if the vehicle replays with a safe data packet and diminished if it replays with a corrupted data packet. This transaction involves two nodes: the first one can be a consumer or a producer. It contributes to the verification of the received packet and thus modifies the rank of the sender. The second one is the packet's sender; it will have an updated rank value after the validation by the first node. The forwarding process of BIoVN is illustrated in Fig. 5. Once a node receives an interest packet, the ID of the sender is verified. If the MVT indexes it, the node drops the packet immediately. Otherwise, the process is continued according to the NDN interest forwarding process.

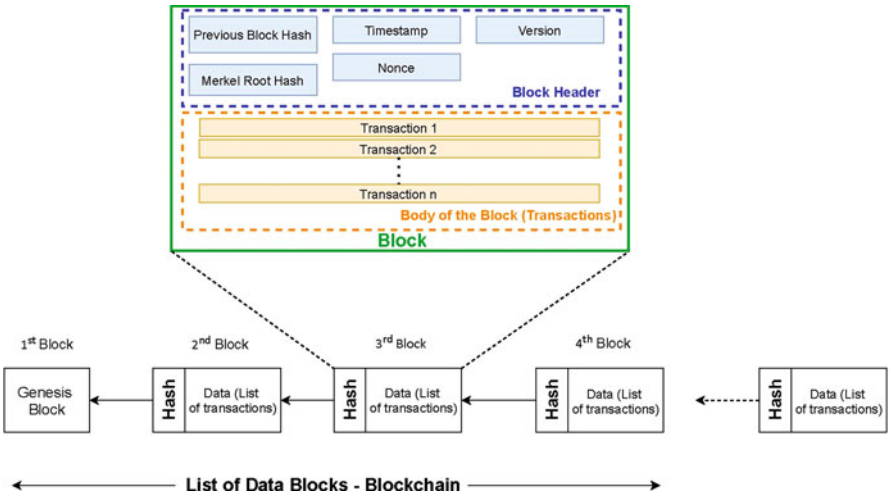

Fig. 4 Design of the blocks

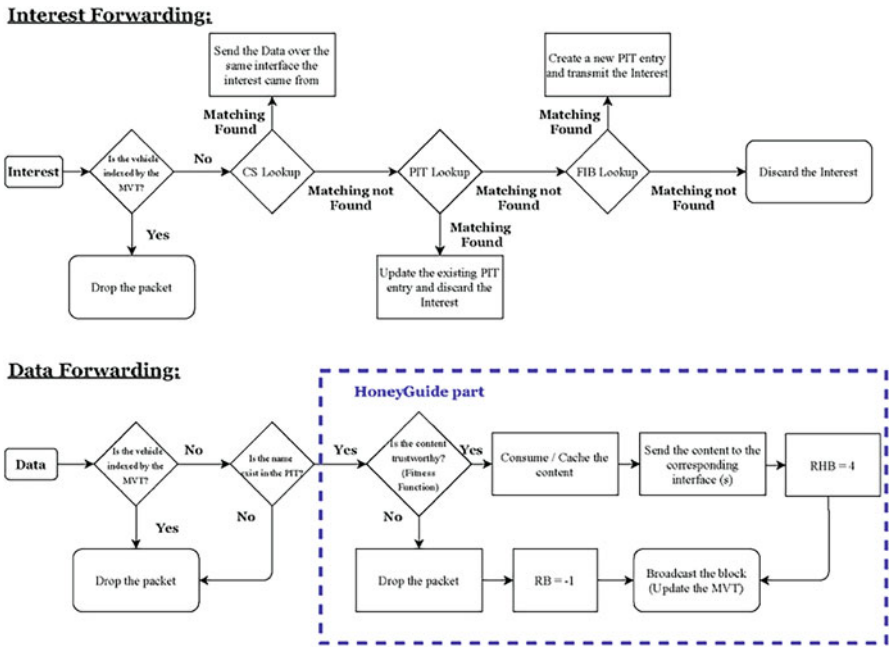

Fig. 5 Forwarding process in BIoVN

Introducing HoneyGuide to Blockchain (Data Forwarding)

The main task of the HG focuses on the update of the MVT. Our required step here is to find the most stable table among introduced nodes by the HG part. An efficient new fitness function is also introduced and used in this phase. The HG algorithm selects the most stable route via intelligent configuration of the fitness function based on the parameter rank R, which will be increased when the fitness function is satisfied and decreased otherwise (refer to Section "HoneyGuide Search Algorithm"). Following that, the table is updated in the second part.

The next step is getting information about surrounding vehicles. Once a vehicle X receives a data packet from another vehicle Y, it sends a request to the blockchain system to get Y's trust level (i.e., the rank R). If Y is found to be recorded in the MVT, X will drop its packet immediately and won't cache it in its CS. Else, if Y is legitimate, its name will not be recorded in the MVT, and X can trust it (see Fig. 5).

The process continues then, and the PIT is verified to ensure that the desired data is already recorded among packets which are not yet satisfied. If it is not the case, the packet is dropped. If it is the case, the packet enters the HoneyGuide part to verify the fitness function. The trustworthiness of the packet is verified based on the served content. If it is fake, the packet is dropped, and the consumer ranks the sender to "-1" and broadcasts the block to the network to update the MVT. If it is authentic, the consumer can consume the content if it is the original requester or caches and forward it to the corresponding interfaces. The consumer then ranks the sender to "4" and broadcasts the block to the network to update the MVT. Figure 6 depicts the basic elements of the BIoVN system.

As a preliminary result, forwarding interest packets in the original VNDN is done without validation. In contrast, in our proposed system, the interest packets are forwarded only if they are valid. In other words, BIoVN discards the packets coming from malicious vehicles, and only the interests coming from vehicles with high ranks are forwarded. It also communicates with the blockchain network about malicious vehicles and reduces their ranks. VNDN also has a significant PIT memory since each interest packet occupies an entry even if it is invalid, which leads to memory consumption compared to BIoVN, which has a miniature table. The same result also can be obtained when it comes to the memory utilization of the CS since VNDN caches all the packets and doesn't reject the invalid ones.

5 Conclusion

The main purpose behind this work was to propose a robust system to secure the Internet of vehicles. In this paper, we proposed a new system that introduces blockchain to NDN. After that, we combined a novel bioinspired algorithm HoneyGuide, with blockchain that we introduced in the data forwarding process. In conclusion, from the outcome of our investigation, we believe that bringing blockchain to the Internet of vehicles over the future Internet architecture named

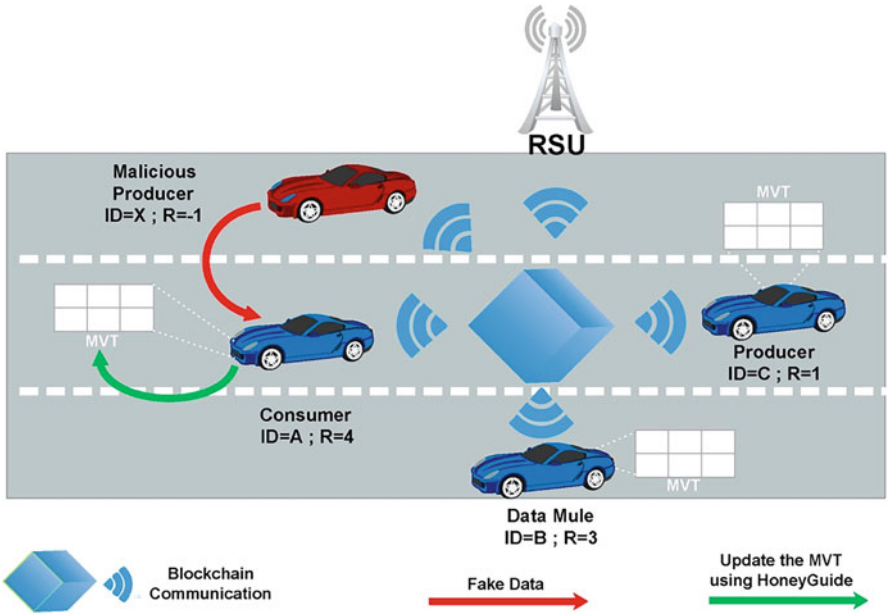

Fig. 6 Basic elements of the BIoVN system

data networking can be considered a great help against security issues faced by vehicular networks. To the best of our knowledge, this is the first work dealing with such a system using blockchain technology and a new bioinspired algorithm. The future work consists of completing the simulation and comparing our system to the original VNDN.

Acknowledgments This research work is supported by the "SafeRoad: Multiplatform for Road Safety (MRS)" Project under contract No: 24/2017, financed by the Ministry of Equipment, Transport, Logistics and Water (METLE), and the National Center for Scientific and Technical Research (CNRST).

References

1. Z. Sabir, A. Amine, A novel system based V2V communications to prevent road accidents in Morocco, in *The 2021 International Conference on Digital Technologies and Applications, Morocco*, (2021)
2. Z. Sabir, S. Dafrallah, A. Amine, A novel solution to prevent accidents using V2I in Moroccan smart cities, in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), UAE*, (2019), pp. 621–625
3. Z. Sabir, A. Amine, PrOMor: A proposed prototype of V2V and V2I for crash prevention in the Moroccan case. Adv. Sci. Technol. Eng. Syst. J **6**(1), 200–207 (2021)

4. Z. Sabir, A. Amine, Connected vehicles using NDN: Security concerns and remaining challenges, in *International Conference on Optimization and Applications (ICOA)-7th Edition, Germany*, (2021)
5. V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, R.L. Braynard, Networking named content, in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, ACM, USA, CoNEXT '09*, (2009), pp. 1–12
6. E. Zhang, J. Burke, S. Thornton, T. Zhang, K. Claffy, P. Massey, W. Abdelzaher, Y. Crowley, Named Data Networking (NDN) project. CAIDA p 27. Technical Report (2010)
7. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang, Named data networking. SIGCOMM Comput. Commun. Rev **44**(3), 66–73 (2014)
8. Z. Sabir, A. Amine, NDN vs TCP/IP: Which one is the best suitable for connected vehicles? in *Recent Advances in Mathematics and Technology, Applied and Numerical Harmonic Analysis*, (Springer International Publishing, 2020), pp. 151–159
9. Z. Sabir, A. Amine, Performance of named data networking in connected vehicles, in *Proceedings of the 4th European International Conference on Industrial Engineering and Operations Management, Italy*, (2021)
10. Z. Sabir, A. Amine, Connected vehicles using NDN for intelligent transportation systems, in *The International Conference on Industrial Engineering and Operations Management, Paris, France*, vol. 2018, (2018), pp. 2433–2441
11. M.F. Bari, S.R. Chowdhury, R. Ahmed, R. Boutaba, B. Mathieu, A survey of naming and routing in information-centric networks. IEEE Commun. Mag. **50**(12), 44–53 (2012)
12. M. Amadeo, C. Campolo, A. Molinaro, Information-centric networking for connected vehicles: A survey and future perspectives. IEEE Commun. Mag. **54**(2), 98–104 (2016)
13. Nakamoto S, Bitcoin: A peer-to-peer electronic cash system (2008). White Paper URL https://bitcoin.org/bitcoin.pdf. Last accessed 2021/03/15
14. Bitcoin, What bitcoin is, and why it matters. (2011). https://www.technologyreview.com/2011/05/25/194486/what-bitcoin-is-and-why-it-matters/. Last accessed 2021/03/15
15. K. Lei, J. Fang, Q. Zhang, J. Lou, M. Du, J. Huang, J. Wang, K. Xu, Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks. J. Grid Comput **18**(4), 593–613 (2020)
16. D.B. Rawat, V. Chaudhary, R. Doku, Blockchain: Emerging applications and use cases. arXiv:190412247 [cs] (2019)
17. M.U. Sattar, R.A. Rehman, Interest flooding attack mitigation in named data networking based VANETs, in *2019 International Conference on Frontiers of Information Technology (FIT), Pakistan*, (2019), pp. 245–2454
18. A. Arsalan, R.A. Rehman, Prevention of timing attack in software de-fined named data network with VANETs, in *2018 International Conference on Frontiers of Information Technology (FIT), Pakistan*, (2018), pp. 247–252
19. V. Jain, R.S. Kushwah, R.S. Tomar, Named data network using trust function for securing vehicular Ad Hoc network, in *Soft Computing: Theories and Applications*, (Springer, Singapore, Advances in Intelligent Systems and Computing, 2019), pp. 463–471
20. P. Manimaran, P ARK, NDNIDS: An intrusion detection system for NDN based VANET, in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Belgium*, (2020), pp. 1–5
21. G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, R. Kumar, A Blockchain framework for securing connected and autonomous vehicles. Sensors **19(14)**, 3165 (2019)
22. R. Shrestha, R. Bajracharya, A.P. Shrestha, S.Y. Nam, A new type of blockchain for secure message exchange in VANET. Digit. Commun. Netw **6**(2), 177–186 (2020)
23. S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, M. Atiquzzaman, A scalable blockchain based trust management in VANET routing protocol. J. Parallel Distrib. Comput **152**, 144–156 (2021)
24. L. Zhang, M. Luo, J. Li, M.H. Au, K.K.R. Choo, T. Chen, S. Tian, Blockchain based secure data sharing system for Internet of vehicles: A position paper. Vehic. Commun **16**, 85–93 (2019)

25. J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J. **6**(3), 4660–4670 (2019)
26. D.B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, C. Kamhoua, Blockchain enabled named data networking for secure vehicle-to-everything communications. IEEE Netw. **34**(5), 185–189 (2020)
27. F. Ahmad, C.A. Kerrache, F. Kurugollu, R. Hussain, Realization of Blockchain in named data networking-based internet-of-vehicles. IT Professional **21**(4), 41–47 (2019)
28. H. Khelifi, S. Luo, B. Nour, H. Moungla, S.H. Ahmed, M. Guizani, A blockchain-based architecture for secure vehicular Named Data Networks. Comput. Electr. Eng **86**, 106715 (2020)
29. M. Dorigo, G. Di Caro, Ant colony optimization: A new meta-heuristic, in *Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), USA*, vol. 2, (1999), pp. 1470–1477
30. D. Teodorovic, P. Lucic, G. Markovic, M.D. Orco, Bee Colony optimization: Principles and applications, in *2006 8th Seminar on Neural Network Applications in Electrical Engineering, Serbia*, (2006), pp. 151–156
31. J. Kennedy, R. Eberhart, Particle swarm optimization, in *Proceedings of ICNN'95 - International Conference on Neural Networks, Australia*, vol. 4, (1995), pp. 1942–1948
32. M. Mitchell, *An Introduction to Genetic Algorithms* (MIT Press, 1998) ISBN 978-0-262-63185-3
33. X.S. Yang, Firefly algorithms for multimodal optimization, in *Stochastic Algorithms: Foundations and Applications*, (Springer, Berlin, Heidelberg., Lecture Notes in Computer Science, 2009), pp. 169–178
34. X.S. Yang, A new metaheuristic bat-inspired algorithm, in *Nature Inspired Cooperative Strategies for Optimization (NICSO 2010), Studies in Computational Intelligence*, ed. by J. R. González, D. A. Pelta, C. Cruz, G. Terrazas, N. Krasnogor, (Springer, Berlin, Heidelberg, 2010), pp. 65–74
35. M. Dhivya, M. Sundarambal, L.N. Anand, Energy efficient computation of data fusion in wireless sensor networks using Cuckoo Based Particle Approach (CBPA). Int. J. Commun. Netw. Syst. Sci **04**(04), 249 (2011)
36. E.R. Speed, Evolving a Mario agent using cuckoo search and softmax heuristics, in *2010 2nd International IEEE Consumer Electronics Society's Games Innovations Conference, China*, (2010), pp. 1–7
37. A. Ouaarab, B. Ahiod, X.S. Yang, Discrete cuckoo search algorithm for the travelling salesman problem. Neural Comput. & Applic. **24**(7), 1659–1669 (2014)