Blockchain enabled Named Data Networking for Secure Vehicle-to-Everything Communications

Danda B. Rawat, Ronald Doku, Abdulhamid Adebayo, Chandra Bajracharya and Charles Kamhoua

***Abstract*—Huge amount of information is expected to be exchanged in vehicular networks through vehicle-to-everything (V2X) communications for enhancing overall traffic efficiency and road safety. However, there are several critical challenges to be addressed before completely realizing the full potential of V2X networking. Privacy-aware security is one of the central components to be addressed for V2X communications. This paper presents a novel framework by leveraging best features of two emerging technologies: blockchain technology and named data networking (NDN) for privacy-aware secure V2X communications. The proposed framework does not use the private information of users (owners, drivers, pedestrians, passengers, cyclists, etc.) in vehicular networks while providing verifiable secure V2X communications by using non-private information such as number plate of the vehicle (like in ParkMobile App or E-ZPass systems use) for integrity and accountability of the communications. Specifically, integrity and accountability in the proposed framework for its users are achieved by amalgamating the best features of blockchain technology and NDN. Furthermore, the proposed approach aims to increase the trust and transparency and reduce the business friction in smart transplantation systems.**

***Index Terms*—Blockchain in vehicle-to-everything (V2X) communications, Named data networking for V2X communications.**

I. Introduction

Vehicular networking for intelligent transportation systems is regarded as a backbone where vehicles are expected to exchange infotainment (information and entertainment) data by using vehicle-to-everything (vehicle-to-vehicle, vehicle-to-pedestrian, vehicle-to-cyclist, vehicle-to-traffic lights, vehicle-to-roadside unit, vehicle-to-cloud/edge) communications, as shown in Fig. 1, for improving overall traffic efficiency and road safety. Upcoming traffic related information can be disseminated to the following vehicles to avoid traffic accidents and congestions through single hop or multi-hop vehicle-to-vehicle communications or vehicle-to-roadside communications. Roadside infotainment messages such as gas price and local attractions can be received by using vehicle-to-roadside communications. In near future, vehicles are expected to make informed decision about their surroundings using their own computing, communications, storage and control engineering systems. Furthermore, each vehicle is expected to broadcast its periodic status information such as traveling speed, direction and geolocation more than eight times a second to its neighbors [1], [2]. Vehicles could process their local information that they have individually and make their decision on the fly, which is good for time critical events. However, this does not address scalability issues for large scale vehicular networks. Furthermore, when individual vehicles work independently, errors could be very high. To provide scalability and minimize errors caused by individual processing and decision making process, vehicles form local clusters with the vehicles who have common interests (such as vehicles traveling in same direction or same lane, vehicles interested to music streaming, etc.) to process their data in a collaborative way and make the decision based on the received information. For instance, vehicle could coordinate with each other and manage to cross the intersection or to take turn left or right in the traffic intersections. However, to get the information about pedestrian or cyclist, vehicles are required to communicate with the roadside units (RSUs) or individual stakeholders such as pedestrian or cyclist to make informed decision about their surroundings. Furthermore, smart vehicles will be producing 25 Gigabytes of data every hour which will be not only challenging to offload this huge data to the cloud but also to process the data locally by each vehicle [2]. Thus, context-aware data offloading could be used to decide which data should be offloaded to the cloud or edge and which part of the data should be processed locally by individual vehicle or cluster of vehicles. In context-aware data offloading, edge server located at each RSU could provide mobile edge computing (MEC) services to provide near-real-time computing for delay sensitive applications. When offloaded data is not time sensitive, cloud computing could process the data and send the processed results back to the vehicles or pedestrians. The data could be stored at cloud servers to provide global view for future use. In all cases, not only the communication overhead in vehicular network is very high but also the privacy-aware secure vehicle to everything communications are not addressed enough to realize its full potential.

To support emerging vehicular networks and address above issues, there have been different approaches proposed in the literature including named data networking (NDN) architecture [3]–[5]. In NDN, name of the content instead of IP address is used where named content is discovered and delivered to the inquirer. NDN offers several benefits to deliver contents in high mobility and intermittent connectivity scenarios in vehicular networks which has challenges in traditional IP-

Manuscript received Day Month Year.

Danda B. Rawat, Ronald Doku and Abdulhamid Adebayo are with the Data Science & Cybersecurity Center (DSC^2), Department of Electrical Engineering and Computer Science at Howard University, Washington, DC 20059, USA. Corresponding E-mail: db.rawat@ieee.org, danda.rawat@howard.edu.

Chandra Bajracharya is with the Department of Electrical Engineering, Capitol Technology University, Laurel, MD, USA.

Charles Kamhoua is with the US Army Research Lab, Adelphi, MD, USA.

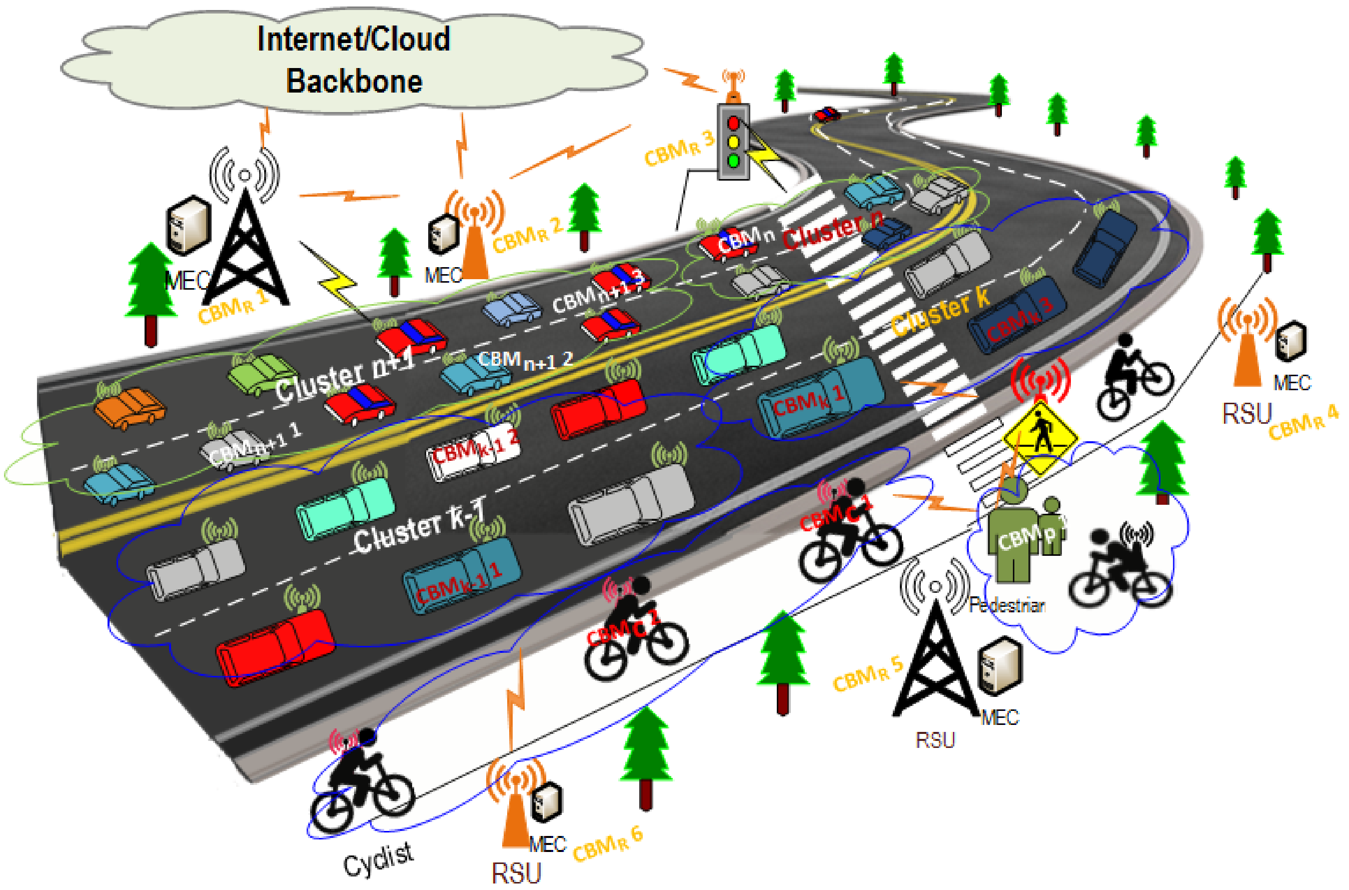

Fig. 1. Typical Vehicle-to-everything (vehicle-to-vehicle, vehicle-to-pedestrian, vehicle-to-cyclist, vehicle-to-traffic lights, vehicle-to-roadside unit, vehicle-to-cloud/edge) communications.

based networks. NDN provides security by operating at packet level and privacy by leveraging the named content instead of identity based contents. NDN has been proposed for vehicular networking [6] that focuses on architecture and data forwarding where security and privacy are rarely investigated.

Furthermore, blockchain – *also known as* distributed digital ledger – technology is widely used for different applications [7]. Blockchain keeps a list of blocks (that have different transactions/operations/data) that are linked with each other using hash values. Blockchain technology provides both integrity and accountability among participating nodes. Thus, it has potential to be used in vehicular networks for secure communications.

In this paper, we propose a joint blockchain and NDN based privacy-aware secure vehicle-to-everything, called Secure-V2X, communication framework. The proposed *Secure-V2X* framework does not use the private information of users (owner, driver, passengers, pedestrian, cyclist, etc) of V2X communications while providing verifiable secure V2X communications by using non-private information such as number plate of the vehicle (like in ParkMobile App or E-ZPass systems) for integrity and accountability of the communications. Furthermore, integrity and accountability in Secure-V2X framework for its users are achieved by using blockchain technology.

The rest of the paper is organized as follows. Section II presents brief overview of blockchain and named data networking. Section III presents the proposed Secure-V2X framework with blockchain and named data networking. Section IV presents performance evaluation. Section V concludes the paper.

II. Overview of Blockchain Technology and Named Data Networking

A. Brief Overview of Blockchain Technology based Security/Privacy and its Limitations

Blockchain is a distributed ledger technology first used by Satoshi Nakamoto for Bitcoin [8]. Blockchain has shown several salient characteristics including trust, security and immutability through chained blocks of transactions using hashes and the privacy through a pair of unique keys (private and public keys) but not using the actual identity of the user. Each user in Blockchain system is identified by a public key. In blockchain based technology, private key is secretly stored in the client device whereas the public key with a dubbed member's ID is distributed to other users to exchange information. Based on [8], [9], getting someone's private key from its public key in blockchain technology is almost impossible which helps to prevent any impersonating attacks in the networked systems. To do a transaction in blockchain enabled systems, client combines recipient's public key and its (i.e., sender's) own private key along with the information that it wants send using a mathematical operation. Then the transaction is broadcast to the entire network for verification by each user by using its public key. This ensures blockchain can reach to a consensus without using any third-party but using a consensus algorithm such as Proof of Work (PoW) [8], [9]. Note that a user/client can change its key, which is the identity in the network, to ensure privacy through anonymity. Blockchain technology has been widely used for different applications [7] including crypto-currency [8], [9]. The authors in [10] argued that blockchain can provide security and privacy in vehicular networks for vehicle to vehicle communications where vehicles are expected to maintain blockchain databases locally to eliminate centralized trusted third-party. Furthermore, blockchain can mitigate the link attack [10] which is a hacker can de-anonymize a user by linking different pieces of data associated with the same anonymous user. Their proposed work does not consider V2X environment [10] which is challenging problem because of diverse set of users in V2X.Furthermore, due to complex consensus algorithm, conventional blockchain used in Bitcoin has some limitations such as system can do up to seven transactions per second [8]. Thus, this approach is not scalable for V2X networking where diverse set of users (cyclist, passengers, pedestrians, RSUs and drivers) are expected to participate in the information exchange process.

B. Brief Overview of Named Data Networking (NDN) Security and its Limitations

NDN uses the named contents instead of network layer packets (IP packets) [3], [4] where NDN named contents are immutable. That is, when users want to change contents, they must generate new names and every named content in NDN has a unique signature generated while binding name and content using its public key (which can be used for securing NDN and for verifying the received data). Note that the NDN security is based on a pair of keys (private and public keys) used by the participating users (such as vehicles, passengers, pedestrians, cyclists and RSUs in our case). A given NDN user has its one or more names and one or more public and private key pairs. For example, for a user named "/41CM3250/MD" based on vehicles number plate (called an identity), the security signature combines its both name and public key together for certifying ownership and key together. Note that use of the number plate of the vehicle (like in ParkMobile App or E-ZPass systems) does not violate the privacy of the user/driver. Through a pair of keys and security signature, users can backtrack and verify the certificates through the certificate chain to the trust anchor. The trust anchor model and trust management can be easily achieved by using a trusted centralized third-party. Once the NDN has the content, the end user can query for the content and get the response back as shown in Fig. 2. However, a trusted centralized third-party based trust anchor system has a bottleneck problem that could easily suffer from denial of service attacks. This issue can be solved by using peer-to-peer based decentralized blockchain technology, which is proposed in this paper.

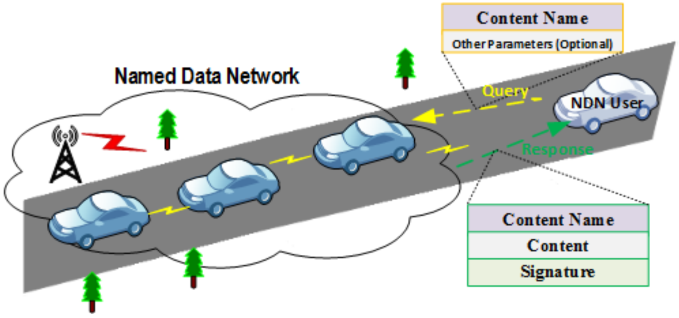

Fig. 2. A typical example scenario with 'a content interest query' and 'a response data packet' for a given client/user in named data networking (NDN). These 'content interest query' and 'response data packet' operations are the transactions in blockchain.

III. Secure-V2X: Blockchain enabled Named Data Networking for Secure V2X Networking

As discussed in previous sections, conventional blockchain used in Bitcoin can do up to seven transactions per second [8] and every vehicle in vehicular networks is expected to communicated at least 8 times a second with its periodic status messages to update its neighbors. Thus, the traditional blockchain approach is not scalable for V2X communications where diverse set of users (cyclist, pedestrians, passengers, RSUs) are expected to participate in the information exchange process.

Thus, we proposed to use V2X framework where individual users (pedestrians, passengers, cyclists) could participate independently or form clusters (of vehicles traveling in same direction or that have same interest) in which a cluster head or a group of cluster heads communicates with the other inter-cluster heads, as shown in Fig. 1. When clustering is used

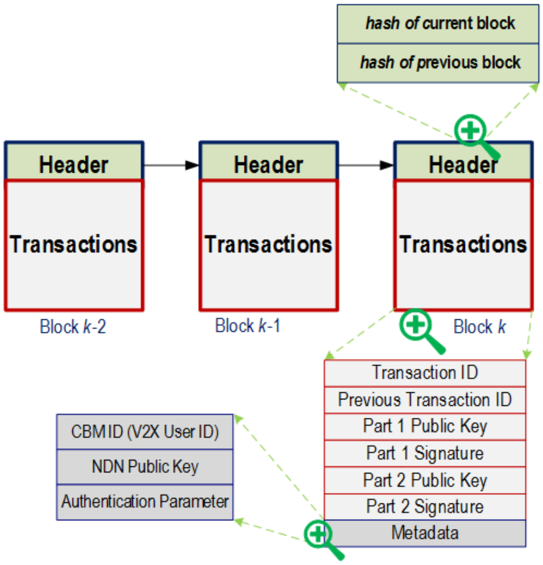

Fig. 3. A typical structure of blockchain with details of a block in 'blockchain and NDN based V2X framework'.

there are more than one cluster heads within the same cluster. Having multiple nodes as cluster heads provides the fault tolerance through redundancy in case of one cluster head leaving the cluster. Cluster heads of a given cluster communicate with each other and update their databased periodically. One of the cluster heads is nominated to communicate with the cluster heads of the other clusters. Users individually or cluster of users use sharding [11] that separates very large databases into smaller parts (called data shards) for fast and easy access. In blockchain based V2X, only cluster heads maintain blockchain and known as cluster block managers (CBMs). Non-cluster heads maintain the state of the blockchain and get the entire copy from CBMs when needed. Transactions in blockchain are verified by the given cluster head designated as a CBM and other cluster heads within the given cluster get the certified copy for fault tolerance or to serve as a CBM when the designated CBM leaves the cluster. Thus, the sharding and multiple clustering (similar to one proposed in [12], [13]) help eliminate the need for a central third-party to address bottle-neck problem. When vehicles, because of travel destination or high mobility, leave a given cluster and join another cluster based on their location proximity by using soft-handover technology (concept along the line of mobile IP [14]). As each vehicle is assumed to be equipped with storage unit along with computing and communications units, it can store privacy sensitive data (such as location) locally and use that private data with an asymmetric encryption (with a public-private key pair) when used to communicate with other vehicles/users. This assumption is valid since a vehicle needs location information of neighboring vehicles but not the identity of each vehicle along with its location to avoid collision or accidents. Furthermore, vehicle owners/users could define which data should be used to communicate with others before starting the application and thus it provides finer control over the sent data. For instance, vehicles do care about other vehicles or pedestrians to avoid collisions and accidents but do not care about their actual identities. Thus the proposed approach is perfect for the V2X framework.

In Secure-V2X framework, all communications (known as transactions in blockchain) are encrypted by using a pair of public-private keys using asymmetric encryption. A typical structure of the blockchain in ‘blockchain and NDN based V2X framework’ is shown in Fig. 3. Users (owners, drivers, pedestrians, passengers, cyclists, vehicles) are authenticated against public keys instead of their actual identifications. Blockchain based vehicular communication offers strong trust, security and authentication that helps mitigate the risk of vehicles being hacked remotely since the information should be verified through blockchain. Thus enhances the safety of the users (owners, drivers, pedestrians, passengers, cyclists, vehicles) while offering enhanced traffic efficiency and road safety.

IV. Performance Evaluation

To evaluate the performance of the proposed Secure-V2X (joint blockchain and NDN based V2X) framework, we used sharding based tool built in NS-3 [12] with different devices with different capabilities (computing, communications and storage capacities) to participate in blockchain based communications. We plotted the blockchain based communication overhead in two scenarios, as shown in Fig. 4: i) each node/user act and communicate individually and ii) nodes form clusters based on their common interests (such as travel direction/lane, similar speed) and only limited number of cluster members serve as cluster heads to communicate with other clusters. We observed that when all nodes are involved in communication in the proposed Secure-V2X, the blockchain based communication overhead for NDN enabled vehicular networks is maximum, as shown in Fig. 4. However, when nodes form clusters and only limited number of cluster members, known as cluster heads, participate in communications with other clusters as well as within the cluster for providing information to non-cluster heads, the blockchain based communication overhead is significantly lower, as shown in Fig. 4. In clustering based approach, when 70% of the cluster members become cluster heads (which means they participate in communications in V2X framework), the communication overhead is close to its maximum, as shown in Fig. 4. We can conclude that when 50% or less cluster members participate in blockchain based communications, communication overhead (information exchange and delay caused by communications) can be reduced by 10% or more, as shown in Fig. 4.

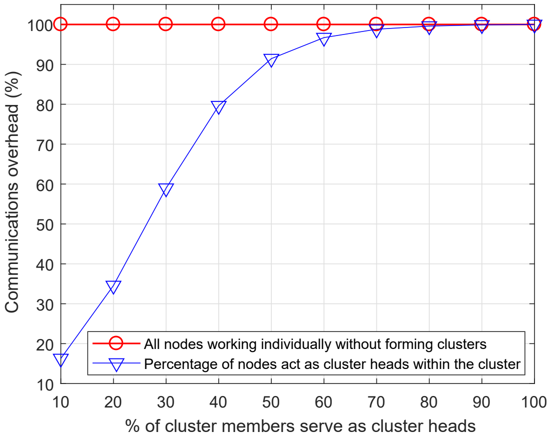

Fig. 4. Variation of communication overhead when all nodes communicate/work independently and when nodes form clusters of common interest but choose % of nodes in the cluster as cluster heads to communicate in the proposed blockchain and NDN based V2X framework.

Next, we plotted the probability of propagating false information vs. the instances of propagating false information in V2X framework, as shown in Fig. 5. This information is used to detect attacks with and without the proposed approach, as shown in Fig. 6. Specifically, we plotted the probability being detected vs. the instances of propagating false information in V2X framework in Fig. 6. Once can observe that when the proposed blockchain enabled NDN is used, the probability of detecting the false information propagation is 100%, which is higher than that of without using the proposed approach, as shown in Fig. 6. However, without blockchain enabled NDN, detection probability increases with increasing instances of lieing, as shown in Fig. 6. The main reason of getting better result with the proposed approach is that blockchain keeps track of all transactions/operations which can be used to detect/track-back any malicious actions in V2X.

V. Open Issues and Research Perspectives

In previous sections, we have provided the Blockchain enabled NDN for secure vehicular communications in V2X environment. However, the proposed fusion of two emerging technologies is the first attempt, thus there are several open issues and research perspectives which are briefly discussed below:

Big data and delay in V2X: The data generated by vehicles or users is expected to be big in terms of volume, variety and veracity. To make informed devision after processing such big data is challenging. Finding the right information in big data is like finding a needle in a haystack. Thus designing the approach that could filter unnecessary data and using context-aware data offloading and computing could help to deal with big data and delay in the proposed framework.

Keys in Blockchain and NDN for V2X: Both Blockchain and NDN use a pair of keys (public and private). It would be easy to use same key pair for both Blockchain and NDN operations. However, to enhance security level in the proposed framework, two different pair of keys can be used. Trade-off of using single pair or different key pairs and their security impact for Blockchain and NDN for V2X framework can be further explored. Another challenge is that how often the non-cluster members of the cluster in V2X should update blockchain database. As we have proposed that there are multiple cluster heads for fault tolerance propose, it will be very interesting to see upper and lower bounds using formal mathematical analysis for the proposed V2X framework.

Finally, the NDN, caching the named data and pulling the named data needs further modification to leverage machine learning techniques in the proposed V2X framework. It will be interesting to investigate machine learning based caching in blockchain enabled NDN.

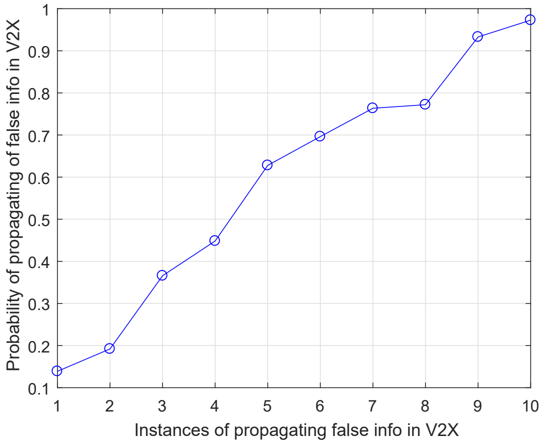

Fig. 5. Probability of propagating false info in V2X framework vs the instances of propagating false info in V2X.

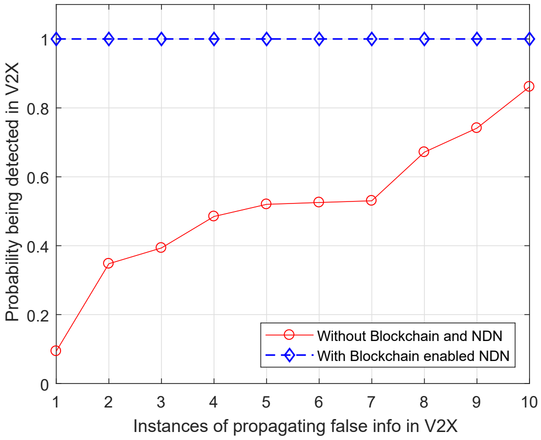

Fig. 6. Probability of propagating false info in V2X framework vs the instances of propagating false info in V2X.

VI. Conclusion

Although vehicular networking offers several benefits for the greater good, it has several critical challenges including privacy and security issues before realizing its full potential. In this paper, we have proposed a novel framework (called Secure-V2X) by leveraging the best features of both blockchain technology and named data networking to address both privacy and security on V2X communications. In Secure-V2X framework, users (owners, drivers, pedestrians, passengers, cyclists, etc.) do not use their private information (unlike in traditional approaches [15]) while providing data integrity, security, privacy and accountability. With the help of proper clustering of users, the proposed Secure-V2X framework helps to enhance the overall network performance while providing privacy-aware secure V2X communications for enhancing traffic efficiency and road safety.

Acknowledgment

This work was supported in part by the U.S. NSF grants CNS-1650831 and HRD-1828811, and by the U.S. Department of Homeland Security (DHS) under grant award number, 2017-ST-062-000003. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies (NSF and DHS).

References

[1] S. Olariu and M. C. Weigle, *Vehicular networks: from theory to practice*. Chapman and Hall/CRC, 2009.

[2] D. B. Rawat and C. Bajracharya, *Vehicular cyber physical systems: Adaptive connectivity and security*. Springer, 2016.

[3] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Communications Surveys & Tutorials*, 2019. to appear.

[4] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang, *et al.*, "Named Data Networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[5] G. Grassi, D. Pesavento, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang, "VANET via named data networking," in *2014 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pp. 410–415, 2014.

[6] S. H. Ahmed, S. H. Bouk, D. Kim, D. B. Rawat, and H. Song, "Named data networking for software defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 60–66, 2017.

[7] D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain: Emerging Applications and Use Cases," *arXiv preprint arXiv:1904.12247*, 2019.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin. org/bitcoin. pdf," 2008.

[9] T. Simonite, "What Bitcoin Is, and Why It Matters," MIT Technology Review, May 25, 2011. URL (accessed 1 January 2019): https://goo.gl/Btqrfc.

[10] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[11] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: A Fast Blockchain Protocol via Full Sharding," *IACR Cryptology ePrint Archive*, vol. 2018, p. 460, 2018.

[12] U. Khakurel, D. B. Rawat, and L. Njilla, "FastChain: Lightweight Blockchain with Sharding for Internet of Battlefield-Things in NS-3," in *2019 IEEE International Conference on Industrial Internet (IEEE ICII 2019)*, (Orlando, Florida, USA), pp. 241–247.

[13] R. Doku, D. B. Rawat, M. Garuba, and L. Njilla, "LightChain: On the Lightweight Blockchain for the Internet-of-Things," in *2019 IEEE International Conference on Smart Computing (IEEE SMARTCOMP)*, pp. 444–448, 2019.

[14] M. Riedel and Y. Xu, "QoS-aware handover procedure for IP-based mobile ad-hoc network environments," Apr. 6 2010. US Patent 7,693,093.

[15] S. Han, S. Xu, W. Meng, and C. Li, "Dense-device-enabled cooperative networks for efficient and secure transmission," *IEEE Network*, vol. 32, no. 2, pp. 100–106, 2018.

Danda B. Rawat (S'07, M'09, SM'13) is an Associate Professor in the Department of Electrical Engineering & Computer Science, Founding Director of the Data Science & Cybersecurity Center (DSC^2), Director of Howard CS-Graduate Programs, and Founding Director of CWiNs Research Lab at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning and wireless networking for emerging networked systems. Dr. Rawat is the recipient of NSF CAREER Award.

Ronald Doku (S'18) has been working towards his PhD in Computer Science under the supervision of Dr. Danda B. Rawat in the Data Science & Cybersecurity Center and Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA.

Abdulhamid Adebayo (S'17) has been working towards his PhD in Computer Science under the supervision of Dr. Danda B. Rawat in the Data Science & Cybersecurity Center and Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA.

Chandra Bajracharya (S'10, M'14) is a faculty member in the Department of Electrical Engineering at Capitol Technology University, USA. Her research interests include cyber-physical systems, smart grid, communication systems, numerical electromagnetic, UWB antenna design and signal processing.

Charles A. Kamhoua (S'10, M'12, SM'14) is a researcher at the Network Security Branch of the U.S. Army Research Laboratory (ARL) in Adelphi, MD, USA, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security.