A TRUST-AWARE CLUSTER-BASED COMMUNICATION ARCHITECTURE FOR VEHICULAR NAMED DATA NETWORKING

Chaker Abdelaziz Kerrache
Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat, Algeria

NOTE: Corresponding author: Chaker Abdelaziz Kerrache, ch.kerrache@lagh-univ.dz

Abstract *– Information-centric Networking (ICN) is a new networking paradigm that aims to solve the problem of the traditional TCP/IP-based Internet. Content-centric Networking (CCN) and Named Data Networking (NDN), both based on the Interest/Data communication paradigm, are two of the most well-known and specialized implementations of ICN. In contrast to typical networks, NDN enables intrinsic security, which ensures data security rather than communication channel security. Each response/data packet in transit has a signature on the contents of the data to ensure security. As a result, an invalid signature indicates an unauthenticated data packet. This ongoing hierarchical authentication verification approach causes a significant delay while providing the appropriate security levels. As a result, in a highly mobile environment with delay-sensitive applications like Vehicular Ad hoc Networks (VANETs), such a technique is neither viable nor scalable. We present a unique Trust-Aware Cluster-based Communication Architecture (TACCA) for Vehicular Named Data Networking in this study, which aims to improve the security of NDN-driven VANETs (VNDN). It separates the route segments into clusters and chooses cluster heads based on their trustworthiness and proximity to the center location. The selected cluster heads are then in charge of disseminating interest packets to prevent the broadcast storm problem. Once the data producer has been located, the data is returned to the requester in the quickest and most secure manner possible. Simultaneously, the intermediate vehicles decided whether or not to verify the data's validity based on their subjective perceptions of the data's producer's conduct. As a result, the calculation complexity and time are reduced. Our idea is able to maintain vanilla NDN security standards while lowering the produced end-to-end latency by more than three times, according to simulation data. As a result, the proposed TACCA is more suited to mobile networks and time-critical applications.*

Keywords – Named data networking, security, trust management, vehicular named data networks, vehicular networks

1. INTRODUCTION

The core of the Cooperative Intelligent Transportation System (C-ITS) is the vehicular ad hoc network (VANET), which uses automobiles as nodes. This type of communication technology not only increases driver safety, but it also improves passenger comfort [1]. Safety applications and entertainment apps are the two broad types of VANET applications. The first category is concerned with road safety, while the second is concerned with value-added services such as traffic information and entertainment (together known as infotainment) on the road. Both of the aforementioned categories' applications are built on cooperative communication and information sharing between C-ITS units, without sacrificing generality. As a result, the majority of VANET applications are content-centric, meaning that the information itself is more significant than the content owner's identify or location. As a result, NDN has lately been recognized to be the architectural backbone for VANET and its derivatives, such as VANET-based clouds and vehicle social networks, thanks to the Future Internet architecture (FIA) [2].

The primary reasons for the slow pace of VANET adoption on a large scale have been security and privacy concerns. To date, research into VANET security challenges has generated positive outcomes; nevertheless, several vulnerabilities still require further examination and remedies. The attacks that target secure content communications, for example, are the most hazardous in ad hoc networks in general and in VANET in particular. Many methods have been offered to guarantee that both safety and comfort messages are sent in a secure and reliable manner. Finding a fair trade-off between security, efficiency, and network needs, however, remains a difficulty. Existing vehicular communication security solutions may be split into two categories: trust-based solutions [3, 4] and cryptography-based solutions [5, 6].

VANET applications have always required data sharing across network entities, independent of the content producer(s) or provider's origin(s). As a result, NDN has the potential to be a significant facilitator for the implementation of VANET applications that not only expand the applications and services domain, but also handle conventional issues like mobility management and security [7]. New security challenges, such as interest flooding, cache poisoning, access control, and data authenticity, are also present in NDN. The deployment of NDN over VANET as an alternative to the traditional TCP/IP communication model has conceived a new hybrid network, which is called Vehicular Named Data Networking (VNDN). The substantial concept of VNDN is to benefit from the NDN prototype, which concentrates on delivering data regardless of its physical location [8, 9]. Most

of the currently available schemes to improve the security of NDN-enabled vehicular networks, dubbed vehicular NDN (VNDN) [10], take the traditional security approaches used in vanilla NDN for fixed or wired network use cases, in which content or data must be signed by the producer, then by the authority that signed the producer's certificate, before moving up the chain of trust until we reach a self-signed network entity (conventionally trusted authority). The needed data dependability is guaranteed by this technique of checking and assuring data authenticity. However, in a highly dynamic environment like the VANET, it results in a significant overhead, which is unsuitable for delay-sensitive and bandwidth-hungry VANET applications. A lightweight communication architecture that respects both NDN security principles and VANET characteristics is required to fill the holes [11]. As a result, the purpose of this research is to present an efficient and lightweight trust-assisted communication method for VNDN, in which data authenticity is supported by trust evaluation.

In this study, we present a novel hybrid communication architecture for VNDN that decreases inter-vehicular communication authentication processing delays and bandwidth usage. For data relayed over the Roadside Units (RSUs), the proposed approach keeps the same vanilla NDN authentication procedure. The suggested architecture separates road segments into clusters, with the selected cluster head responsible for the dissemination, collection, and forwarding of interest packets to the next cluster. A cluster head is a trusted entity, and when these entities are chosen, the current trust level of the candidates is taken into consideration. In other words, the cluster head is chosen based on the trust value and the distance to the cluster's center, at least in part. Cluster heads are more likely to be chosen if they have a high trust value and are near to the cluster's center point. When a node requests content and produces interest in it, the demand finally reaches the node with the content in its CS (either it is the owner of the content or has received the content during past communications). The material will be sent to the requester through the quickest and most reliable path available at this time. Because the data producer and consumer's locations are already known, they may be readily localized using the GLS, which is a location service for geographic ad hoc routing.

We minimize this overhead by evaluating the data producer's trust after the inter-vehicle trust is established through evaluation of historical inter-vehicle communications. Instead of authenticating the chain of trust or web of trust (which is both time consuming and inefficient), we evaluate the data producer's trust. As a result, the producers are categorized according to their level of trust. We can do probabilistic authenticity verification for trustworthy producers, in which the validity of a portion of the material created by that producer is reviewed and certified, but for non-trusted nodes, the legitimacy of every chunk of the information is verified. It is also worth mentioning that when the producer's trust rating rises, the number of verifications decreases, resulting in improved performance. Furthermore, each producer's trust is controlled. Finally, the authentication procedure is automatically incorporated with the intermediary routers until the content reaches the RSU for data arriving from the vanilla NDN in fixed or wired networks, thus there is no need to check it again. As a consequence, the authentication time is reduced and the VANET's real-time applications are supported.

Contributions of the paper are summarized as follows:

- A new trust-based communication architecture is proposed for VNDN.
- A lightweight data authentication strategy is used over the established inter-vehicle trust.
- A unicast-based data delivery technique through the shortest most trust path is proposed.
- Extensive simulation tests are performed to prove the validity and performance of the proposed scheme with respect to the existing solutions.
- The future research and open challenges posed by this merger of technologies are also discussed.

The rest of the paper is organized as follows: in Section 2, we present the data authentication process used by the vanilla NDN. Section 3 describes our proposed trust-aware cluster-based authenticated communication architecture for VNDN. The performance evaluation of our proposed architecture is discussed in Section 4 followed by open security challenges in VNDN in Section 5. Section 6 concludes the paper with future directions.

2. VANILLA NDN DATA AUTHENTICATION

Communications in vanilla NDN involves two types of packets (i) Interest packet that requests the content from the network and contains the name of the requested content. Interest packet consists of various fields such as `Name`, `Nonce`, `Selectors`, `InterestLifeTime`, and `ForwardingHint`. `Name` and `Nonce` are mandatory fields in an interest packet, whereas the rest of the fields are optional. `Selectors` are used to find the best match within the available data with the requested data in the interest. (ii) As a response to the interest packet, a data packet containing the actual requested material is sent. Unlike the interest packet, which uses a forwarding mechanism to search the network for the requested content, the data packet is returned unicast, and the data owner must sign each packet to establish the material's validity.

Every node in the vanilla NDN (a specific implementation of NDN) maintains the following three data structures:

- Content Store (CS): Every node maintains a local cache memory to store the received content from other nodes. This node may be the requester or the intermediate relayer along the path. Due to CS, the local availability of content guarantees increased performance and reduces the delay.

- Pending Interest Table (PIT): PIT stores all the interests that a router has forwarded but not yet satisfied.
- Forwarding Information Base (FIB): It is a routing table matching the requested data name with its correspondent interface.

NDN delivers inherent security by securing the data rather than the communication route (as in the traditional networks). Each piece of material is signed by the creators. Intrinsic security eliminates the resource-intensive sophisticated methods necessary for communication security while also making authenticated data available locally in the CS. As a result, the majority of data-related assaults are automatically prevented. The signature of a data packet includes two primary fields: the signature type (usually SHA-256 with RSA) and the KeyLocator, which defines the name of the producer's public key and refers to another data packet holding the certificate or public key required to validate the signature value. Because the certificate is an NDN data packet, it includes its own Signature field. Fig. 1 shows the format of an NDN data packet.
Authentication of a data packet in NDN is done in a hierarchical manner. For example, if a node gets a VANET course written by author "A" and published in the blog "LIM," the authentication of this packet is done as follows:

1. Check the signature of the author.
2. Check the signature of the blog administrator who certified the author.
3. Check the authority who certified the blog administrator. This latter, is generally a trusted self-signed authority, such us Google or Yahoo.

The data packet is regarded legitimate if the entire key chain can be verified, as shown in Fig. 2.

3. PROPOSED TRUST-AWARE CLUSTER-BASED AUTHENTICATED COMMUNICATION ARCHITECTURE FOR VNDN

The fundamental goal of this project is to develop confidence among communication vehicles. Second, split the road segments into clusters, with the cluster heads chosen so that their trust values are the highest and they are as close to the cluster's core locations as feasible, as in [12]. Third, take use of the clusters that have established to prevent the broadcast storm that may be produced by the spread of interest packets. It's worth emphasizing that the cluster heads are in charge of disseminating the interest packet to the remainder of the cluster. The farthest front and rear cars serve as relay nodes for intra-cluster communications. Fourth, after the data producer or a node with a copy of the requested data is located, the data packet is sent back to the requester vehicle over the quickest and most trusted way, as described in [13]. Finally, the data authentication process is carried out based on how trustful is the producer of this data. Figure 3 summarizes our proposed TACCA architecture.

The proposed inter-vehicle trust establishment and administration are presented in the following sections, followed by a lightweight data authentication based on inter-vehicle trust.

3.1 Vehicle-to-vehicle trust establishment

Inter-vehicle trust between vehicles i and j has two main metrics: (a) Interaction-based trust ($DirectT^{t_x}_{(i,j)}$), and (b) recommendation-based trust ($IndirectT^{t_x}_{(i,j)}$) in a specific time period t_x. Every vehicle continuously monitors the network to evaluate the honesty of nearby vehicles. The overall trust $Trust(i,j)$ is then computed by combining both Interaction-based and recommendation-based trusts. We also use factors $1-\frac{1}{\#act+1}$ and $\frac{1}{\#act+1}$ in such a way that the more direct interactions we have, the more we consider the interaction-based trust than the recommendation-based one, and vice-versa. Since vehicles may be in the communication range of each other several times, over several time periods, we consider the average direct/indirect evaluation during these periods. However, if a nearby RSU broadcasts an evaluation about a specific vehicle, its evaluation is considered instead of the inter-vehicle trust.

The global inter-vehicle trust of vehicle j is computed by vehicle i using the following equations:

In the absence of RSU:

Trust(i,j)=

$$1-\frac{1}{\#act+1}\cdot\left[\frac{\sum_{x=1}^{m} DirectT^{t_x}_{(i,j)}}{m}\right]+\frac{1}{\#act+1}\cdot\left[\frac{\sum_{x=1}^{n} IndirectT^{t_x}_{(i,j)}}{n}\right] \quad (1)$$

In the presence of RSU:

$$Trust(i,j) = RSU_{Eval}(j) \quad (2)$$

According to Eq. *(2)*, In the absence of RSU, the content is received from neighbors, and either direct or indirect trust is employed to validate the content's validity, but in the presence of RSU, content authenticity is verified via the standard NDN technique.

The following subsections discuss the details of the direct $DirectT$ and the indirect $IndirectT$ trusts' computations.

3.1.1 Interaction-based trust (Direct)

interaction-based trust of vehicle j evaluated by vehicle i, is the ratio of the forwarding actions, $DirectT(i,j)$, to the total number of actions (both drops and forwards) during time t_x, m. It can identify forwarding-related attacks including blackholes, grayholes, and Denial of Service (DoS) assaults. Interaction-based trust should be defined differently for different adversary models.

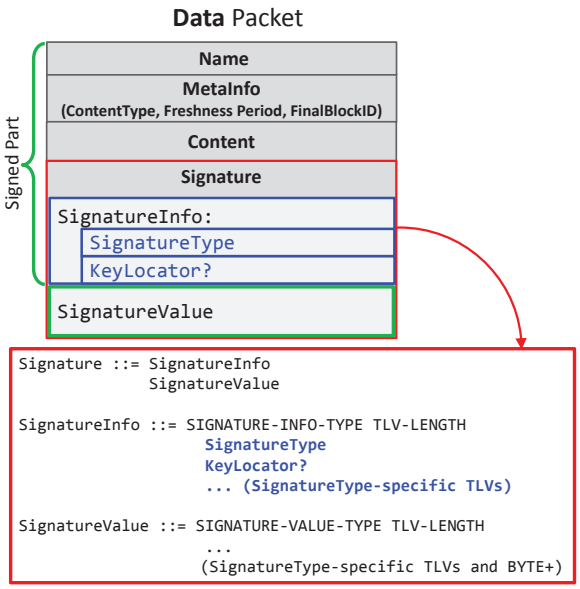

Fig. 1 – Format of NDN data packets.

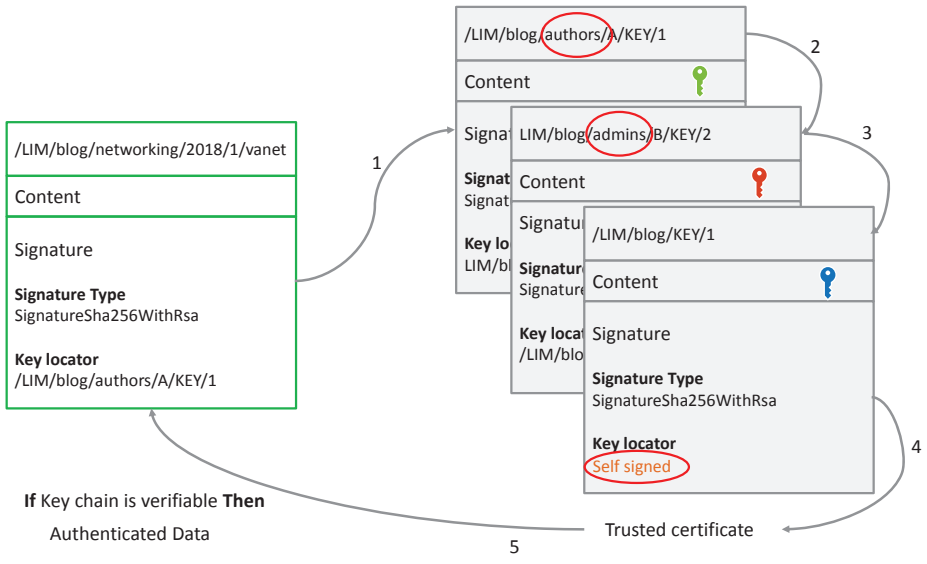

Fig. 2 – Vanilla NDN data authentication process.

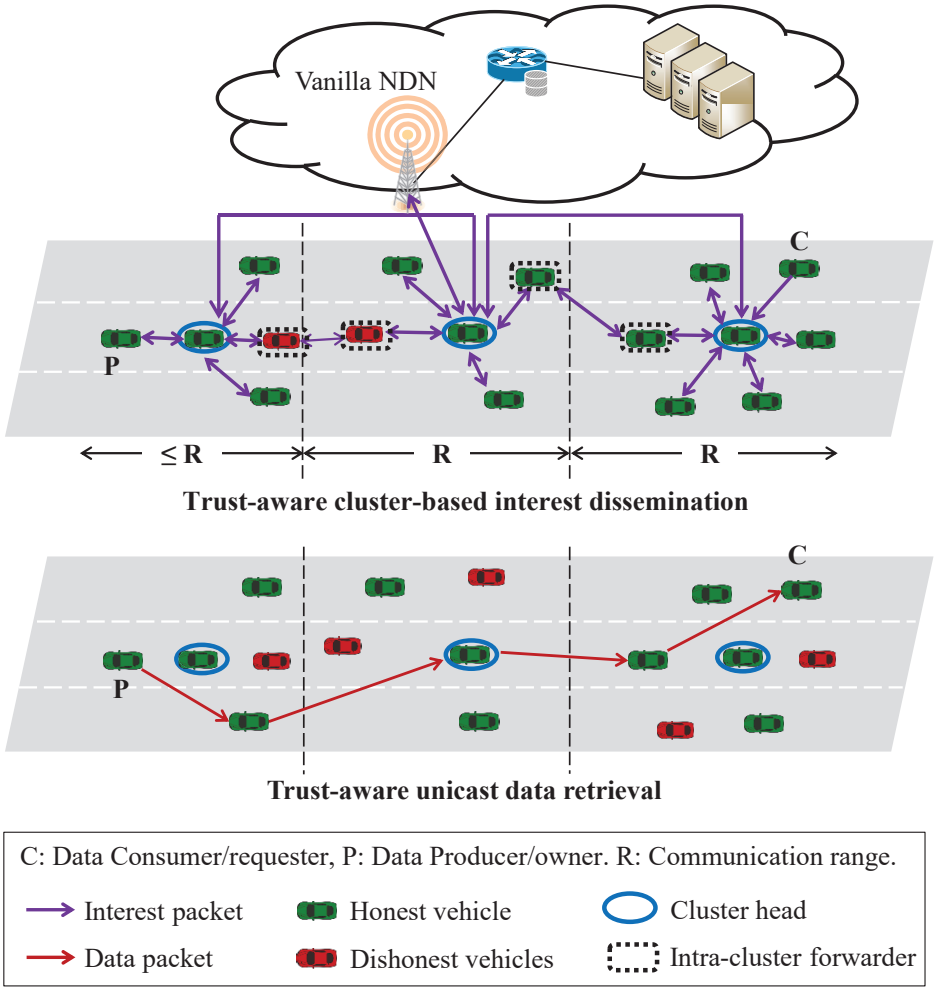

Fig. 3 – Proposed trust-aware cluster-based communication architecture.

3.1.2 Recommendation-based trust computation (Indirect)

Usually, the vehicles exchange recommendations (Indirect trust denoted by $IndirectT^{t_x}_{(i,j)}$ in Eq. *(2)*) when there is no prior knowledge about the behavior of a specific vehicle. These recommendations can be sent either as on-demand recommendation messages or together with the exchanged data messages. The opinion of the trusted recommender (let say vehicle k) concerning the behavior of another vehicle j, is combined with the direct trust of the recommender k during a time period t_x. When we have recommendations from n neighbors, we can take an average of the recommendation as shown in Eq. *(2)*. The term trusted recommender refers to the fact that the recommending node itself is trustworthy.

3.2 Proposed trust-based data authentication mechanism

Trusted self-signed authorities are always reachable in vanilla NDN. As a result, determining the legitimacy of a data packet is always possible. However, due to mobility and network dispersion, such a time-consuming method is not possible in VANETs. Additionally, this method has a negative impact on the performance of real-time and delay-sensitive VANET applications. To solve these issues, we offer a technique that checks data authenticity using existing trust between nodes. The level of trust built aids in selecting whether to skip the authenticity check and accept the data as is.

In order to assure utmost confidence in the received data, the standard vanilla NDN authentication method is retained in VNDN for data originating from an untrusted vehicle. However, content validity is frequently reviewed offline for trustworthy cars, and the more the producer's confidence, the longer the duration of forwarding without verification. Finally, data from the RSU is automatically authenticated using the standard NDN protocol. As a result, there is no need to verify the data validity of previously authorized data via the wired portion of the link. Fig. 4 summarizes our proposed adaptive authentication process. In the figure, vehicle B has a lower trust value (not trusted), therefore data received from B must be authenticated every time it is received by node A.

4. PERFORMANCE EVALUATION

To evaluate performance of our proposed TACCA scheme, we relied on the VNDN daemon implemented in the NS-2 simulator considering the IEEE 802.11p standard. In our simulations, we considered the Citymob mobility model [14] and the mobility traces are generated using SUMO [15]. The topology region considered in the simulations is of 5 km^2, which is equally divided into the 6×6 grid map, and the vehicular velocity is varying in the range of [0, 20] meters per second. The results are average of 10 simulation runs, where in each run 10 requesting vehicles or consumers generate interests at the rate of 20 interests per second. In addition to that, 4 data producers and two malicious vehicles are considered in each scenario. Those malicious vehicles inject unauthenticated data when they receive the interest packet. The consumer and producer vehicles are randomly chosen in every run. The total simulation duration is $600\ sec$ and the consumers generate interests during the whole simulation duration.

4.1 Performance metrics

TACCA performance evaluation is done through two security-related metrics and two network-related metrics, which are described below:

- *Detection ratio (%)*: This represents the ratio of the number of detected unauthenticated data packets to the total number of received unauthenticated data.
- *False Positive (FP) ratio (%)*: The FP represents the number of data packets that are detected as unauthenticated while its not the case, to the total number of detected unauthenticated data.
- *Average end-to-end delay (s)*: This represents average time between sending the interest packet and receiving content as a result of the request for all connections.
- *Content Delivery Ratio (CDR) (%)*: CDR means the number of successfully fulfilled interest packets to the total number of generated interests.

First, we evaluate the suggested TACCA trust-based data authentication method to the typical vanilla NDN data authentication technique, as well as the produced false positives. Following that, we look at their capacity to handle delay-sensitive applications, where the average end-to-end latency and the CDR are measured.

4.2 Results and discussion

The ratio of identified unauthenticated data packets in relation to time for both TACCA and NDN authentication schemes for 100 and 300 cars density is shown in Fig. 5. The resulting curves demonstrate that for low density, both techniques have a lower detection efficiency than for a large density, indicating that the vanilla NDN strategy is always better. The TACCA approach, on the other hand, exhibits nearly the same outcomes as the NDN technique over a short amount of time (needed to create confidence between cars).

Furthermore, Fig. 6 depicts the produced false positive, which reveals that, with the exception of the beginning of the studies when inter-vehicle trust had not yet reached its stable levels, the created false positive for both NDN and TACCA is almost identical. The trust-based data authentication technique of TACCA maintained almost the same performance as the vanilla NDN strategy, as seen in both figures.

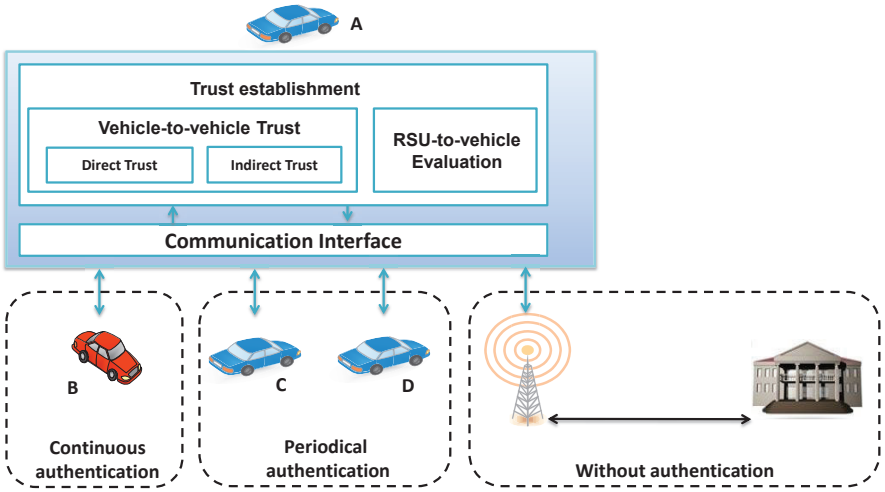

Fig. 4 – Proposed trust-based data authentication mechanism.

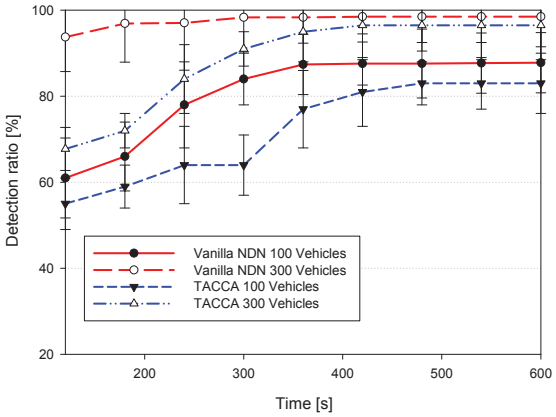

Fig. 5 – Detection ratio of unauthenticated data packets for both TACCA and vanilla NDN.

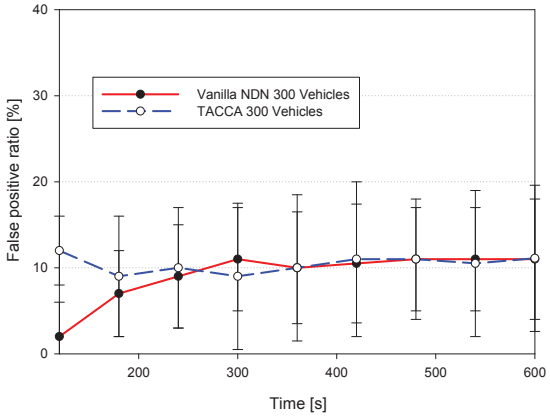

Fig. 6 – Generated false positive during the detection of the unauthenticated data packets for both TACCA and vanilla NDN.

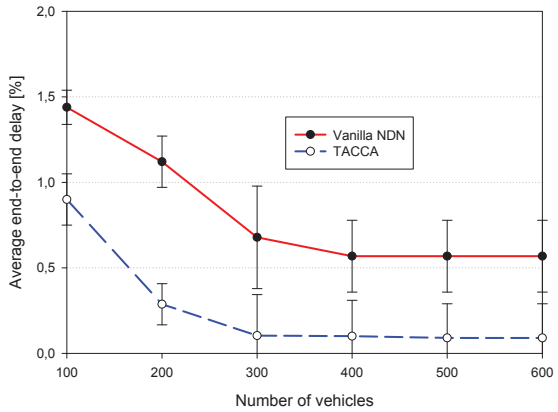

Fig. 7 – Average end-to-end delay for both TACCA and vanilla NDN forwarding strategies.

The average end-to-end latency of data packets is shown in Fig. 7, which demonstrates that our approach decreases the delay by more than 300 percent when compared to vanilla NDN for 300 cars density. In low density scenarios, however, this improvement is roughly 80%. (i.e., 100 vehicles). As a consequence of the findings, TACCA beats vanilla NDN, making it more appropriate for real-time ap- plications as well as other VANET applications.

The packet delivery ratio for both TACCA and vanilla NDN forwarding techniques is shown in Fig. 8. It shows that the TACCA trust-aware forwarding approach beats vanilla NDN forwarding solutions in both low and high density scenarios offering more than 9% improvements for low density cases and up to 40% for the high densities, with virtually optimum results in the high density case.

5. CHALLENGES IN VNDN SECURITY

Interest flooding, cache poisoning, and key management issues were all included in the design of vanilla NDN. Because data/content must be signed by the producer and

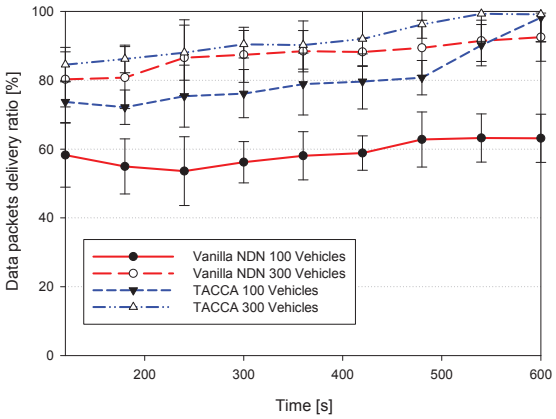

Fig. 8 – Packet delivery ratio for both TACCA and vanilla NDN forwarding strategies.

then hierarchically by the authorities who signed the producer's certificate, it implicitly ensures three basic security features: data integrity, correctness, and source authentication, and thus provides data-centric security rather than communication channel security. In this article, we look at a few security problems in VNDN that need to be looked at further [16].

5.1 Efficient key and identity management

Existing research has only looked at the efficiency of currently used signature algorithms (such as SHA256 with RSA, ECDSA, or HMAC). However, few studies have looked at the issue of certificate distribution, revocation procedures, and pseudonyms shifting in order to protect producers' data privacy. Furthermore, in VNDN, usually a trusted authority may not always be approachable. So, how will the data's veracity be verified? To determine the viability of the currently existing schemes in VNDN, a more thorough examination is required [17].

5.2 Network performance

Vanilla NDN now operates via IP, and NDN packets are already incorporated in lower layers with their own security measures. The network performance would be harmed as a result of this double verification for authorized data. More information is needed to address this issue so that the bottom layer can skip data authenticity when necessary. As a result, the security techniques for the present NDN are still being investigated [18].

5.3 Data security

Because data packets are signed but not encrypted, data secrecy cannot be guaranteed. For the time being, we'll assume that the requested data is freely available; however, if the data is encrypted, the consumer should be supplied with key management and access to that data depending on their access privileges. Another issue is the content store, where the material might be stored in encrypted form but the metadata would still be in cleartext. As a result, greater research into access to NDN's encrypted data is required. Because of the mobility and intermittency of cars in VNDN, this problem is particularly acute [19].

5.4 Access control

One of the most critical requirements in VNDN is access control. When customers express an interest in data, it should be examined to see if they have access permissions to that information. Another significant consideration is the entity in charge of validating access rights: should it be the publisher or an intermediary node? In wired networks, such verifications are normally handled by intermediate routers; however, in mobile networks like VNDN, this security issue necessitates further examination [20].

5.5 Trust management

Unlike standard TCP/IP-based VANET trust management, which divides trust into entity-based, data-based, and hybrid trust models, VNDN only supports data-based trust models by default. As a result, in VNDN, effective data trust management mechanisms are required. Because the data trust must be tied to the publishers/producers, the entity trust cannot be fully ignored in VNDN; yet, owing to mobility and intermittent connectivity, monitoring trust levels for individuals would entail significant expense. As a result, a viable alternative must be devised. Furthermore, the duration of trust is an area that requires deeper exploration. Context-aware trust management schemes, in which the trust parameters are updated based on the context of the application, may perform better in VNDN, depending on the type of application. To this end, both delay-sensitive and delay-tolerant applications must be taken into account while working with trust [21].

5.6 Trust bootstrapping and propagation

Bootstrapping is another issue that has to do with trust. On their initial encounter, nodes are usually given an average value, however this may not always reflect the node's true behavior. As a result, neighbors should communicate historical information about the nodes in order to assess trust. Furthermore, trust propagation will be difficult in VNDN because to the potential for an increased network overhead. The piggybacking strategy, on the other hand, may be examined to see if it is effective in VNDN trust propagation [22].

5.7 Auditing and incentives

Cooperation between surrounding nodes is required for trust propagation and recommendation. This propagation becomes difficult in resource-constrained and intermittent contexts, and convincing neighbors to suggest this becomes tough. Incentives might be imple-

mented like in traditional networks to encourage active engagement of neighbors for recommendation; however, the communication paradigm of NDN advocates for new methods to control incentives and the audit of incentives. In this area, more study is required. To summarize, VNDN is a viable communication paradigm for implementing ITS applications and services; but, security and privacy concerns must be thoroughly researched and solved before it can be commercialized [23].

6. CONCLUSIONS AND FUTURE WORK

Despite vanilla NDN's success, security and privacy concerns must be addressed. Other challenges have arisen as a result of the inherent security concept of NDN and its offshoots, such as VNDN, such as the overhead paid by hierarchical data authenticity. In theory, hierarchical data authenticity prevents all sorts of man in the middle attacks, but it comes at the cost of significant computational, memory, and latency overhead, which are often undesirable in highly mobile networks like VANET. We propose a new Trust-Aware Cluster-based Communication Architecture (TACCA) for vehicular named data networking to fill in the gaps. To circumvent the broadcast storm problem during interest propagation, our suggested solution uses a trust-aware clustering technique. TACCA employs inter-vehicle trust to determine whether or not to verify data authenticity for a certain node without compromising the intended security levels. TACCA's efficiency in maintaining vanilla NDN security levels while minimizing the overhead was demonstrated through simulation results. The primary open problems in VNDN security were also covered in the report.

We intend to focus our future research on data privacy and caching regulations. Furthermore, new VANET data transmission research relies on the usage of unauthenticated/unauthorized and energy-restricted Unmanned Aerial Vehicles (UAVs) in crucial scenarios such as disaster management and rescue applications. As part of our future study, we intend to explore the reliability of the data supplied by these VNDN-To-UAV communications.

REFERENCES

[1] George Dimitrakopoulos and Panagiotis Demestichas. "Intelligent transportation systems". In: *IEEE Vehicular Technology Magazine* 5.1 (2010), pp. 77–84.

[2] Man Wan and Shiqun Yin. "Future internet architecture and cloud ecosystem: A survey". In: *AIP Conference Proceedings*. Vol. 1955. 1. AIP Publishing LLC. 2018, p. 040130.

[3] Farhan Ahmad, Fatih Kurugollu, Chaker Abdelaziz Kerrache, Sakir Sezer, and Lu Liu. "Notrino: a novel hybrid trust management scheme for internet-of-vehicles". In: *IEEE Transactions on Vehicular Technology* 70.9 (2021), pp. 9244–9257.

[4] Chaker Abdelaziz Kerrache, Carlos T Calafate, Juan-Carlos Cano, Nasreddine Lagraa, and Pietro Manzoni. "Trust management for vehicular networks: An adversary-oriented overview". In: *IEEE Access* 4 (2016), pp. 9293–9307.

[5] Haowen Tan and Ilyong Chung. "Secure authentication and key management with blockchain in VANETs". In: *IEEE access* 8 (2019), pp. 2482–2498.

[6] Rasheed Hussain, Donghyun Kim, Junggab Son, Jooyoung Lee, Chaker Abdelaziz Kerrache, Abderrahim Benslimane, and Heekuck Oh. "Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds". In: *IEEE Internet of Things Journal* 5.4 (2018), pp. 2441–2448.

[7] Boubakr Nour, Hatem Ibn-Khedher, Hassine Moungla, Hossam Afifi, Fan Li, Kashif Sharif, Hakima Khelifi, and Mohsen Guizani. "Internet of things mobility over information-centric/named-data networking". In: *IEEE Internet Computing* 24.1 (2019), pp. 14–24.

[8] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, Yasir Faheem, Rasheed Hussain, and Adlen Ksentini. "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges". In: *IEEE Communications Surveys & Tutorials* 22.1 (2019), pp. 320–351.

[9] Hakima Khelifi, Senlin Luo, Boubakr Nour, and Sayed Chhattan Shah. "Security and privacy issues in vehicular named data networks: An overview". In: *Mobile Information Systems* 2018 (2018).

[10] Xiaonan Wang and Yanli Li. "Vehicular named data networking framework". In: *IEEE Transactions on Intelligent Transportation Systems* 21.11 (2019), pp. 4705–4714.

[11] Chaker Abdelaziz Kerrche, Farhan Ahmad, Mohamed Elhoseny, Asma Adnane, Zeeshan Ahmad, and Boubakr Nour. "Internet of vehicles over named data networking: current status and future challenges". In: *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks*. Springer, 2020, pp. 83–99.

[12] Rashmi Ranjan Sahoo, Rameswar Panda, Dhiren Kumar Behera, and Mrinal Kanti Naskar. "A trust based clustering with Ant Colony Routing in VANET". In: *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*. IEEE. 2012, pp. 1–8.

[13] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, and Abderrahmane Lakas. "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs". In: *Vehicular Communications* 9 (2017), pp. 254–267.

[14] Francisco J Martinez, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. "Citymob: a mobility model pattern generator for VANETs". In: *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*. IEEE. 2008, pp. 370–374.

[15] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. "SUMO–Simulation of Urban MObility". In: *The Third International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain*. 2011.

[16] Ahmed Benmoussa, Abdou el Karim Tahari, Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Abderrahmane Lakas, Rasheed Hussain, and Farhan Ahmad. "MSIDN: mitigation of sophisticated interest flooding-based DDOS attacks in named data networking". In: *Future Generation Computer Systems* 107 (2020), pp. 293–306.

[17] Hao Liu, Rongbo Zhu, Jun Wang, and Wengang Xu. "Blockchain-Based Key Management and Green Routing Scheme for Vehicular Named Data Networking". In: *Security and Communication Networks* 2021 (2021).

[18] Joao M Duarte, Torsten Braun, and Leandro A Villas. "MobiVNDN: A distributed framework to support mobility in vehicular named-data networking". In: *Ad Hoc Networks* 82 (2019), pp. 77–90.

[19] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, Syed Hassan Ahmed, and Mohsen Guizani. "A blockchain-based architecture for secure vehicular Named Data Networks". In: *Computers & Electrical Engineering* 86 (2020), p. 106715.

[20] Syed Hassan Ahmed, Safdar Hussain Bouk, Muhammad Azfar Yaqub, Dongkyun Kim, Houbing Song, and Jaime Lloret. "CODIE: Controlled data and interest evaluation in vehicular named data networks". In: *IEEE Transactions on Vehicular Technology* 65.6 (2016), pp. 3954–3963.

[21] Farhan Ahmad, Chaker Abdelaziz Kerrache, Fatih Kurugollu, and Rasheed Hussain. "Realization of blockchain in named data networking-based internet-of-vehicles". In: *IT Professional* 21.4 (2019), pp. 41–47.

[22] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, KC Claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. "Named data networking". In: *ACM SIGCOMM Computer Communication Review* 44.3 (2014), pp. 66–73.

[23] Ezedin Barka, Chaker Abdelaziz Kerrache, Rasheed Hussain, Nasreddine Lagraa, Abderrahmane Lakas, and Safdar Hussain Bouk. "A trusted lightweight communication strategy for flying named data networking". In: *Sensors* 18.8 (2018), p. 2683.

AUTHOR

Chaker Abdelaziz Kerrache is an associate professor at the department of Computer Science, University of Laghouat, Algeria. He is currently the head of the Informatics and Mathematics Laboratory (LIM) at the University of Laghouat. He received his MSc. degree in computer science in 2012, and his Ph.D. degree in computer science in 2017, both at the University of Laghouat, Algeria. In 2013, he joined the Informatics and Mathematics Laboratory (LIM) as a research assistant and the Computer Networks Group (GRC) in 2015 as a visiting PhD student. His research activity is related to trust and risk management, secure multi-hop communications, vehicular networks, Named Data Networking (NDN), and UAVs.