Security of communication 5G-V2X: A proposed approach based on securing 5G-V2X based on Blockchain

Boughanja Manale[1], Tomader Mazri[2]
[1,2]Advanced Systems Engineering, Electrical Engineering, Networks and Telecommunications System, Ibn Tofail Science University, Kenitra, 14070, Morocco
[1]boughnja.manale@gmail.com, [2]tomader20@gmail.com
*Boughanja Manale

Abstract— **With the rapid evolution of wireless communication and autonomous vehicles, vehicle to Everything (V2X) communications provides driving safety, traffic efficiency, and real-time traffic information in-vehicle networks. V2X has evolved by integrating 5G cellular access technology and New Radio (NR) into V2X communications (i.e., 5G NR V2X). Since the security issue in 5G-V2X remains a crucial point, we conducted a literature review approach and identified the 5G-V2X communication levels in this paper. The main objective of this study was to develop an approach to secure 5G-V2X. The proposed methodology is based on Blockchain to ensure the 5G-V2X architecture levels.**

Keywords—Security; 5G---V2X; style; Blockchain

I. INTRODUCTION

Vehicle-to-everything, commonly referenced as "V2X", has been widely addressed in LTE Evolution technology since 2015 and has been increasingly becoming a significant focus of the 3GPP Release 14 standard [1]. Release 14 is commonly referred to as LTE-V, LTE-V2X, or cellular V2X [1]. While the original specification allowed for non-autonomous 5G radio systems to be incorporated into previous generation LTE networks, the scope of Release 15 expands to cover "autonomous" 5G, with a new radio system completed by a next-generation core network. In addition, 5G-V2X can enhance reliability, under certain conditions, by introducing redundant packet delivery. A summary term has also recently been proposed: "C-V2X" or Cellular V2X. This new technology could enhance the development of intelligent transportation systems (ITS) and complement the various existing standards of the last decade proposed by standards development organizations (SDOs), such as IEEE, ETSI[2], and CEN/ISO. Even though V2X communications offer safety and environmental benefits, and 5G supports several requirements[3], such as the connection density to handle millions of requests and links across the square mile, continuous end-to-end latency, the traffic volume density due to several tens of terabytes created every second per square mile, maximum mobility, and throughput, network efficiency the continuous improvement and the multiplication of applications have led to the development of new uses, notably that of connected objects. Some security and privacy issues concerning the 5G and even the V2X.

In this article, we start with the architecture of the 5G V2X. We then exam the trust, security, and privacy issues in the 5G V2X architecture, which is exposed to a variety of cyberattacks, ranging from denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and eavesdropping attacks, to special attacks aiming to corrupt a property of V2X communications, such as the inference attack and identity revealing attack that compromise the privacy of vehicles. To address these trust, security, and privacy issues, extensive and comprehensive analyses of potential strategies are presented in a hierarchical architecture of 5G-V2X [4]. Finally, we offer the proposed solution to secure 5G V2X. To this end, this article is organized as follow: section 2 an overview of 5G-V2X, where we will discuss the architecture and the security issue in 5G-V2X, then in section 3, we will present some solution made to deal with the security issue, and we will present our proposed approach in section 4, finally, we will conclude in section 5.

II. 5G-V2X OVERVIEW

A. 5G-V2X architecture

The 5G system architecture supports two modes of operation for V2X communication, namely V2X communication on the reference point or PC5 interface and V2X communication on the reference point or Uu interface. The PC5 interface supports SL V2X communications for NR and LTE. V2X communications over Uu for UL and DL transmissions. In Release 16, 3GPP sets out improvements for the V2X architecture, embedding V2X services in the 5G architecture, as shown in Figure 1 (in red the main elements supporting V2X) from [5] [6]. The main functions and benchmarks supporting V2X are[7]:

- PC5: the reference point between UEs for V2X communication. V2X communication on PC5 supports LTE and/or NR radio[3];
- Uu: the reference point between the UEs and the NG-RAN node. V2X communication on Uu supports LTE and/or NR radio;
- PCF (Policy Control Function): provides the V2X configuration (radio parameters, QoS, etc.) for V2X

communication via PC5/Uu to V2X devices via control plane signaling (NAS signaling);

- NWDAF (Network Data Analysis Function): provides QoS analysis information to improve V2X communication over Uu;
- The User Plane Function (UPF) is one of the Network Functions (NF) of the 5G Core Network (5GC). The UPF is responsible for packet routing and forwarding, packet inspection, QoS management, and external PDU session for data network (DN) interconnection in the 5G architecture[8];
- The management function (AMF) receives all the connection and session information from the user.

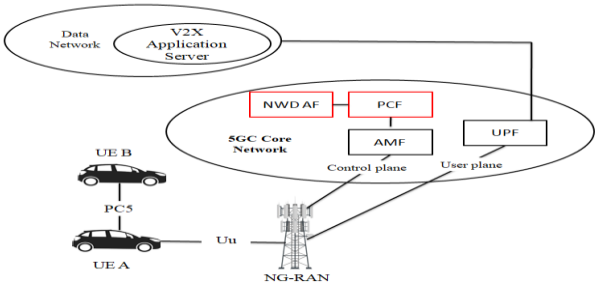

FIGURE 1. 5G-V2X ARCHITECTURE

B. *Security issue in 5G-V2X*

As 5G is currently being defined regarding guidelines, it faces several challenges in its deployment. The new radio (NR) will need constant enhancement of security. In this specified situation, mobile and monitored security services are one of the most heightened areas of progress to react to the digital security challenges inherent in computerized change for communication service providers and their customers. In addition, 5G is engaged in reshaping services and advancing development by offering extended transfer speed, advanced multi-tenant processing, and some creative services, high-content data networks, and high-bandwidth connectivity for machine learning and artificial intelligence (AI). Service assurance in 5G V2X needs ground-breaking, versatile, and collaborative security. With the deployment of 5G V2X come several security threats [9]. We can divide the security issues into general and specific issues. We can divide the security issue for 5G-V2X into two main categories. General and particular issues.

1) *General issues:*

Here, we will provide an overview of several key attacks and threats when deploying services over 5G-V2X[4]:

- Inconsistent gNB placement is the counterpart of eNB and MME of LTE-V2X. The main effect may be the authentication and permission required for a vehicle. The latter then advocates the capture of its certificate to have secure communication between the RSU and the other entities in the network ;
- The existence of a malicious node can exploit the vulnerability of the OBU and gain access to the network (zero-day attacks). Thus, it is the responsibility of the network entity to prevent such attacks. Static information and weak hash functions can lead to certificate forgery. What prevents the capture of secure elements of a vehicle is an ultimate requirement;
- For 5G-V2X, it is advisable to provide good encryption in data sharing to prevent any unwanted third party from taking advantage of the shared information;
- Network planning and configuration, side-channel attacks are tedious to detect and can exploit the entire network by simply affecting the vehicle or gNB in the 5G configuration. In addition to that, service-based attacks are expected to prevail in 5G-V2X, unlike DSRC or LTE-V2X, as all content in 5G must be classified into multiple services. Thus, attack prevention and service-based threat detection are key issues securing 5G-V2X capabilities.

2) *Specific issues:*

5G-V2X bring with it several problems, particular regarding the security requirement; in this subsection, we will detail these particular issues[10]:

- Attacks against availability: attacks centered on data availability are the most dangerous in V2X communication because they impact the primary conditions of well-being. We can find such attacks as a jamming attack which is an interfering radio attack that can be carried out through any communication based on wireless technology ;
- Data integrity attack: when the assailant intercepts the data. The attacker can launch GPS spoofing or even replay attacks;
- Attack on confidentiality: As an essential security feature in V2X communication, all data sent in V2X must be kept secure. An attack such as eavesdropping and location tracking is initiated in the network to break the V2X secrecy;

- Attack on authenticity: guaranteeing authenticity involves checking that nodes access the network using certificates and digital signatures based on their identity. Some threats that violate this requirement are certificate replication, where nodes use replicated certificates that have been blacklisted. In addition, Sybil attacks where one node (the attacking node) pretends to be multiple identities in the road network;
- Non-Repudiation Attack: involves the actual node ID executing a particular behavior.

III. RELATED WORK

The security of 5G V2X communication poses a significant security challenge. For this purpose, a safety enhancement layer must be added to reinforce the security, and the communication must fulfill the CIA (confidentiality, integrity, and availability) requirement. We must first define the distinction between normal and abnormal behavior before starting. An abnormal node may send wrong information to mislead other nodes as it may change the vehicle ID, etc. This section will present the literature on different security solutions implemented into the 5G V2X communication to enhance safety and security.

The author in [10] proposed a lightweight and secure navigation system for VANET. Each vehicle implies a cryptographic and digital signature to handle the process of securely mapping the vehicle to the roadside unit (RSU). The main objective of the SVN is to maintain the integrity and authentication of the message sent by the vehicle to the RSU. An alternative solution was provided by [11], which consists of a reliable and intelligent transfer protocol employing double encryption for data packets and enforcing robust checking schemes to evaluate the node's trust. [12] also suggested a new mechanism that depends on a unique and trusted identity-based asymmetric collection key consent to build cryptographic mixing zones that oppose misleading eavesdropping. In [13], the suggested solution used a support vector machine-based IDS to supervise the system to prevent replay attacks. The solution was made to ensure the communication protocol between different entities in the network is kept safe. A two-dimensional anti-jamming communication methodology for cognitive radio networks is being developed. A secondary user (SU) takes advantage of both spread spectrum and user mobility to cope with jamming attacks while avoiding interference with the primary users. By employing a deep Q-network algorithm, this scheme identifies whether to recommend that the SU leave an area of high interference and chooses a frequency hopping pattern to overcome intelligent jammers [14]. DL-based multiscale time framework is based on choosing feasible interfacing arrangements of neighboring vehicles and reserving boundary design of the joint V2V network. They articulated the optimization problem for resource allocation and proposed the deep reinforcement learning approach with the multi-time scale framework to solve this problem [15]. The proposed solution concentrates on hierarchical privacy preservation among all VANET entities. They presented a reliable and standard CPA secure GS solution to a vehicular network application by accounting for revocability, linkability, and robustness of openness [16]. The DMN algorithm isolates nodes with abnormal behavior and improves network performance. In addition, it optimizes the selection of node behavior. The proposed DMN algorithm assumes three parameters. Based on these parameters, a decision value is evaluated and compared to the verifier selection threshold to isolate malicious nodes [17]. The proposed solution is in the form of an IDS based on compartmentalized attacks. Intrusion detection and decision-making are performed at the cluster members, cluster leaders, and RSUs to eliminate any security threat that may disrupt the network in a short period. AECFV has proven its ability to detect various attacks in the network [18]. In this section, we have presented many applications and solutions implemented to ensure the security of 5G V2X communication to preserve and maintain the security of users. And we have been able to gather these solutions and summarize them into three categories[19]:

- Identity-based cryptography (IBC): the concept of IBC is a cryptographic scheme that is very appropriate for devices with limited computing resources. It has been discussed in many papers to encrypt and sign exchanged messages efficiently;
- Behavior-based: The concept is quite simple; this solution is based on the performance of the attached vehicles communicating in the network and the messages transmitted by the RSU ;
- Machine Learning (ML) based: This predicts threats and attacks based on suspicious network activity and anomaly detection. ML implementation enables automation, adaptability and allows efficient orchestration and dynamic provisioning for large-scale network resource cognition and mobility prediction.

IV. PROPOSED APPROACH

In the earlier section, we provided a detailed architecture of 5G-V2X (Figure 1). Our study found that the attack window decreases, and the protection against threats can be increased. Hence, the security of 5G-V2X represents a critical role [19]. For this fact, security solutions and possible remedies for identified and unidentified threats should be able to handle 5G-V2X implementation approaches and meet the security requirements. We have initiated our work with a level analysis in 5G-V2X, which can be summarized as follow:

- Vehicle security: this level consists of the protection of the vehicle itself, it is mandatory to ensure the link that connects the communication between the UE (vehicle) and, specifically, the PC5 link;
- Authentication of the driver: authentication is a critical point in 5G-V2X communication to ensure that operations are secure and that we send the data to the right recipient;

- Architecture security: in the 5G-V2X concept, the vehicle acts as a BTS for several entities. However, in the case of an attacker's presence, this can cause multiple exploits, especially if the attacker has taken control of the vehicle. In this case, the security of the architecture is a critical point, especially when we are talking about an environment in permanent movement;
- Organization and detection of traffic anomalies: intrusions into such a network can come from multiple sources: speed management, traffic information, road behavior, network, etc. Ensuring that 5G-V2X is secured by a system capable of detecting all kinds of attacks will be beneficial.

From our analysis, we were able to identify four levels in the 5G-V2X architecture that can be retrieved into endpoint, access network, 5G core network, and data network. The figure below shows the four tiers of the 5G-V2X approach:

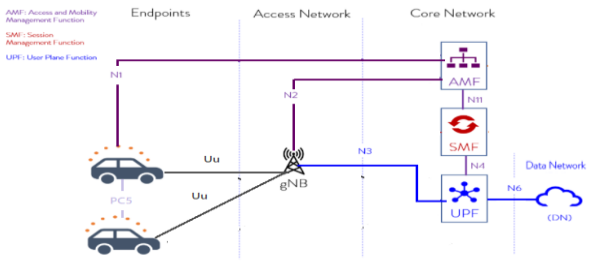

FIGURE 2. 5G-V2X LEVELS

Where: N3: Interface between the RAN (gNB) and the (initial) UPF., N6: Interface between the Data Network (DN) and the UPF, N4: Interface between the Session Management Function (SMF) and the UPF

From figure 2, we were able to perform a general analysis that allowed us to extract the most critical levels for securing the 5G-V2X architecture, which can be summarized in two main levels: Level 1; endpoint, core, and access network security, and level 2, the data storage security. The proposed solution uses the Blockchain concept to enhance the safety of the overall architecture.

A. Concept of the proposed architecture:

The proposal is to engender a scheme that guarantees the trustworthiness of nodes and messages transmitted in 5G-V2X. We will focus on implementing the blockchain process to secure the communication in our network. The proposed approach is based on placing the vehicles in a public Blockchain to serve as a ground of truth for other automobiles. The purpose of the transaction modification is to provide the relevance of 5G-V2X system capabilities to ensure the security of critical information delivery and solve 5G-V2X problems. The adaptive variation method adds new blocks based on event messages, similar to bitcoin transactions, outside the hash sequences of blocks to be connected in chronological order to the Blockchain. This system ensures scalability and speed of message distribution by implementing a local Blockchain with independent chains from different geographical regions. A public Blockchain is supposed to store and manage all the reliability information of nodes and messages provided in a geographical region. A simple Blockchain would not suit the 5G-V2X problem addressed in this study. Therefore, a type of improvised Blockchain mechanism with some functionality adaptation is proposed as a solution. Figure 3 represents the improvised packet structure with Blockchain integration used for secure communication by 5G-V2X components. Each block consists of vehicle i (Vi), vehicle i identity (IDi), message (Mi), timestamp (ti), hash value (hi), misbehavior report, and vehicle status. Security event messages are used here, where Blockchain is the trusted medium for event messages in 5G-V2X.

$Block_i$	V_i	ID_i	M_i	T_i	H_i	Mis_rep_i	$Statut_i$

FIGURE 3. PROPOSED PACKET STRUCTURE WITH BLOCKCHAIN INTEGRATION

The Blockchain integration into 5G cellular technologies enables next-generation vehicular networks to deliver secure vehicular network orchestration, intelligent asset management, trust administration, and enhanced privacy. The proposed solution provides safe and reliable communication over the network. In addition, it also integrates an unsigned public key infrastructure to preserve the privacy of network participants. As a result, it improves the security and privacy of users and messages communicated in 5G-V2X by addressing malicious attacks that intend to have disastrous impacts on the network and other end users. The ongoing expansion of data in 5G-V2X through the implementation of the above technique tends to affect the lightweight functionality of the system over time. The following figure shows the overall proposed approach of the system concept of the proposed solution, in which communication occurs between two vehicles. Four different blockchains were considered for the system design: the Certificate Blockchain (CertBC), the Revocation Blockchain (RevBC), the Message Blockchain (MesBC), and the Trust Blockchain (TrustBC). These blockchains are administered by government agencies, such as the Law Enforcement Agency (LEA) and the Certificate Authority (CA). The standard submission regulations are to be defined by the government agencies and followed by the respective vehicle manufacturers authorized in the country for the participation of their vehicles.

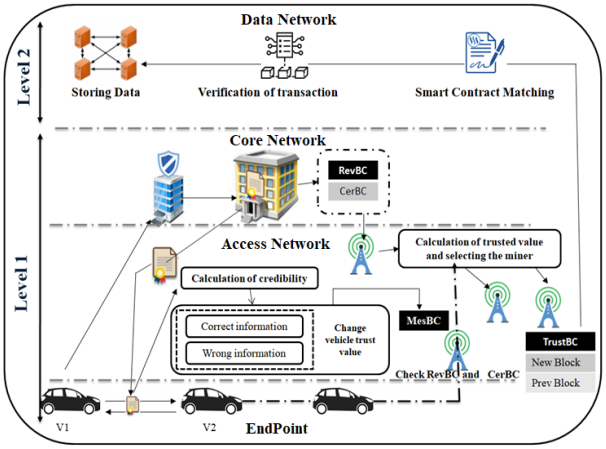

FIGURE 4. PROPOSED BLOCKCHAIN ARCHITECTURE IN 5G-V2X

After explaining the design of our architecture, we will carry out this proposal on our analysis, i.e., implement our solution on the two levels extracted from our analysis (level 1 and 2). The proposed approach is used to verify vehicles in the network. The scheme of our proposal will be as follows: It starts with the initialization of the system where a key pair (public key and private key) is generated, then the Certification Authority (CA) grants a certificate to the vehicle. Once the CA has given the certificate to the vehicle, it goes through an authentication phase where we validate the certificate expiration day and the certificate. The next step is message generation, where the vehicle tries to transmit a message to another vehicle. Once the RSU receives the message, it calculates the trust value offset for each vehicle. Then we start the election of miners and the generation of blocks. After calculating the trust value (hash value), we move to the election of miners and the generation of blocks. This step is the most important for good efficiency because it involves the Blockchain technology in the network. Each RSU in the network stores its timestamp and calculates the hash value. The trust value must not be less than the threshold to validate the RSU as a miner. As an RSU miner, he is regularly elected in the network to manage the Blockchain due to the decentralized structure of Blockchain technology. The election of the RSU miner ensures that the data on the Blockchain is updated quickly. When the miner is selected, the next step is to validate the transmitted message and add it to the Blockchain. The process will be repeated until the end of the message generation. If the sent message is not valid, the block will not be added to the chain and will stop the communication; if not, the block is added, securing the communication levels in 5G-V2X.

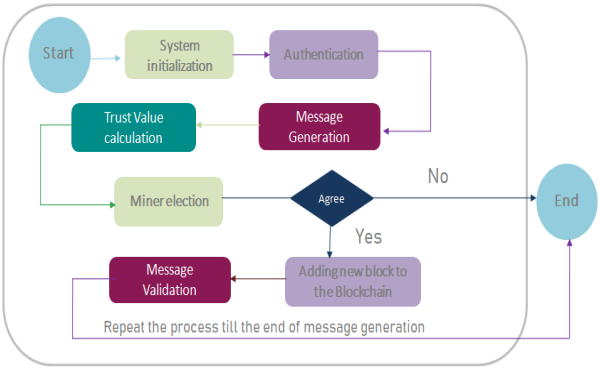

FIGURE 5. THE PROPOSED APPROACH

V. CONCLUSION:

To conclude, mobile communication security is a critical and indispensable point. In this paper, we presented a methodology based on Blockchain that will improve the security of 5G-V2X networks. The study that we conduct in this paper helps us understand the levels of the 5G-V2X architecture and will be very helpful to average readers to have a global idea about security to the 5G-V2X. The conducted methodology will give a secure environment in the 5G-V2X communication. However, to reap the full benefits of this integration, it is essential to address some challenges and identify potential solutions, such as the block length generated. This challenge yet interesting which will be part of our future work.

REFERENCES

[1] E. Universal and T. Radio, "LTE Overall description ;," vol. 0, p. 148, 2009.

[2] M. Iwamura, "NGMN view on 5G architecture," *IEEE Veh. Technol. Conf.*, vol. 2015, 2015, doi: 10.1109/VTCSpring.2015.7145953.

[3] B. Bertenyi, R. Burbidge, G. Masini, S. Sirotkin, and Y. Gao, "NG Radio Access Network (NG-RAN)," *J. ICT Stand.*, vol. 6, no. 1, pp. 59–76, 2018, doi: 10.13052/jicts2245-800x.614.

[4] T. Yoshizawa and B. Preneel, "Survey of Security Aspect of V2X Standards and Related Issues," *2019 IEEE Conf. Stand. Commun. Networking, CSCN 2019*, pp. 1–5, 2019, doi: 10.1109/CSCN.2019.8931311.

[5] A. Festag, "Cooperative intelligent transport systems standards in Europe," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 166–172, 2014, doi: 10.1109/MCOM.2014.6979970.

[6] F. Perry and A. V. Program, "Overview of DSRC messages and performance requirements," 2017.

[7] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G Vehicle-to-Everything Services: Gearing up for Security and Privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389,

2020, doi: 10.1109/JPROC.2019.2948302.

[8] T. Specification, "LTE; User Equipment (UE) to V2X control function; protocol aspects; Stage 3 (3GPP TS 24.386 version 15.0.0 Release 15)," vol. 0, pp. 0–34, 2017.

[9] Patil VP, "Reactive and Proactive Routing Protocol Performance Evaluation for Qualitative and Quantitative Analysis in Mobile Ad Hoc Network," *Int. J. Sci. Res. Publ.*, vol. 2, no. 1, pp. 2250–3153, 2012, [Online]. Available: www.ijsrp.org.

[10] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[11] S. Ur Rehman, M. A. Khan, T. A. Zia, and L. Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges," *J. Wirel. Netw. Commun.*, vol. 2013, no. 3, pp. 29–38, 2013, doi: 10.5923/j.jwnc.20130303.02.

[12] L. Zhang, "OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 12, pp. 2998–3010, 2017, doi: 10.1109/TIFS.2017.2730479.

[13] Q. G. Fan, L. Wang, Y. N. Cai, Y. Q. Li, and J. Chen, "VANET Routing Replay Attack Detection Research Based on SVM," *MATEC Web Conf.*, vol. 63, pp. 4–7, 2016, doi: 10.1051/matecconf/20166305020.

[14] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, Jun. 2017, pp. 2087–2091, doi: 10.1109/ICASSP.2017.7952524.

[15] L. T. Tan and R. Q. Hu, "Mobility-aware edge caching and computing in vehicle networks: A deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10190–10203, 2018, doi: 10.1109/TVT.2018.2867191.

[16] M. S. I. Mamun, A. Miyaji, and H. Takada, "A multi-purpose group signature for vehicular network security," *Proc. - 2014 Int. Conf. Network-Based Inf. Syst. NBiS 2014*, pp. 511–516, 2014, doi: 10.1109/NBiS.2014.93.

[17] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in vehicular ad-hoc networks," in *Procedia Computer Science*, 2015, vol. 46, pp. 965–972, doi: 10.1016/j.procs.2015.01.006.

[18] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Electr. Eng.*, vol. 43, pp. 33–47, 2015, doi: 10.1016/j.compeleceng.2015.02.018.

[19] B. Manale and T. Mazri, "5G, Vehicle to everything communication: Opportunities, constraints and future directions," *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 6, pp. 1089–1095, 2020, doi: 10.25046/aj0506132.