Lightweight and Secure Authentication Model for Vehicle to Everything (V2X) Communication Based on 5G Networks

Meriem Houmer[1,*], Safaa Laqtib[2] and Siham Eddamiri[3]

[1]*Higher school of technologies, Ibn Zohr University, Dakhla, Morocco*
[2]*Informatics and Applications Laboratory (IA), Department of Mathematics and Computer Science, Faculty of Sciences, Moulay Ismail University, Meknes, Morocco*
[3]*Department of Mathematics and Computer Science, University Moulay Ismail, ENSAM, Meknes, Morocco*
E-mail: houmer.m@gmail.com; laq.safaa@gmail.com; sihameddamiri@gmail.com
[*]*Corresponding Author*

Received 22 November 2021; Accepted 14 January 2022;
Publication 05 April 2022

Abstract

Integrating the cellular network infrastructure into Intelligent Transport Systems (ITS) received attention from the research community and standards groups. This technology allows the invention and development of new applications, as well as the development of new vehicle mobility solutions and the enhancement of driver mobility in terms of safety, reliability, capacity, and quality. Cellular communications networks such as LTE-V2X and 5G NR, integrated into the Vehicle to Everything (V2X) architecture designed to support vehicular communications and deployed on a large scale, appear in particular to be a relevant solution. They could indeed guarantee reliable geographic distribution and acceptable performance (latency, bandwidth, packet loss). In this context, we propose a secure authentication scheme for 5G-based V2X communication. To achieve security requirements, our

Journal of Mobile Multimedia, Vol. 18_5, 1399–1424.
doi: 10.13052/jmm1550-4646.1854

approach aims to provide a high degree of security in different vehicular communication (V2V, V2I, V2N) by using lightweight cryptographic algorithms in order to safely receive all keys and messages from RSU, vehicles, and the network. To validate our approach, we use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to achieve the security goals, also evaluate the performance according to the operational cost which demonstrates that our model has a less computational cost.

Keywords: ITS, security, V2X, vehicular communications, 5G, AVISPA.

1 Introduction

In recent years, the automotive industry has become more reliant on wireless communication technologies to satisfy safety requirements. Intelligent Transportation Systems is a novel idea dedicated to the promotion of transportation systems (ITS). ITS is the use of multiple technologies (electronics, telecommunications, data processing, and management) to modernize the interfaces between the vehicle, the driver, and the road. ITS encompasses a wide range of topics in which wireless communications play a critical role. As a result, manufacturers are becoming dedicated to equipping their automobiles with wireless communication capabilities. Because people's beings are prioritized by all stakeholders, traffic safety systems must meet two important requirements: speed and dependability, which must be satisfied by the underpinning communication network [1].

Over the past decade, the connected vehicle paradigm has aroused great interest from academia, governments, industry, and standards organizations. The interaction between the vehicle and the road environment is at the heart of many ITS applications; this requires the development of efficient Vehicle to Everything (V2X) communication systems and higher precision positioning systems. V2X encompasses Vehicles to Infrastructure (V2I) communication, Vehicle to Vehicle (V2V) communication, and Vehicles to Network (V2N) communication [2].

Cellular networks are another technique being studied for vehicle communication network implementation. These cellular networks offer a significant advantage over ITS-G5 networks in that they already have a huge installation that ensures high availability. They can also offer enough transmission rate and latency. High-performance vehicle communications might be deployed using two generations of cellular communications networks: 4G networks (LTE-V2X) and 5G networks [3].

It is crucial that the information exchanged between the various actors of the V2X system is reliable and exact in order to guarantee a certain number of objectives such as authentication, integrity, confidentiality, and privacy. In this context, we propose a secure and lightweight scheme for 5G-based V2X communication in different types of vehicular communication namely V2V, V2I, and V2N. In our solution, we use Elliptic-Curve Cryptography (ECC) and Attribute-based Signature (ABS) to ensure the security of keys and messages exchanged between vehicles or vehicles and RSU, in the other side we consider an improved version of authentication and key agreement protocol based on Elliptic Curve Diffie Hellman (ECDH) for 5G system to surmount standard authentication protocol 5G-AKA limitation. The aim to use elliptic curves and attributes algorithms is their faster processing compared to others cryptographic methods. However, in vehicle-to-infrastructure communication, each vehicle is authenticated with RSU without a trusted third-party authority, and in vehicle-to-network communication, the authentication process and key agreements are established between vehicles, AMF/SEAF, AUSF, and UDM/ARPF.

The rest of the paper organization is as follows. In Section 2, we discuss the 5G technology and the emergence of V2X in the context of vehicular communication. Section 3 presents the security challenges and requirements of V2X. The related work is presented in Section 4. Section 5 describes the different steps of our scheme. We analyse the security and performance evaluation in terms of the operational cost of our proposed in Section 6. Finally, we provide conclusion in Section 7.

2 Background

2.1 5G Characteristic, Architecture and Security Issues

In telecommunications, 5G is the fifth-generation technology standard for broadband cellular networks, which cellular phone companies began deploying worldwide in 2019, and is the planned successor to the 4G networks which provide connectivity to most current cell phones. 5G networks are predicted to have more than 1.7 billion subscribers worldwide by 2025, according to the GSM Association. Like its predecessors, 5G networks are cellular networks, in which the service area is divided into small geographical areas called cells. All 5G wireless devices in a cell are connected to the Internet and telephone network by radio waves through a local antenna in the cell. The main advantage of the new networks is that they will have greater

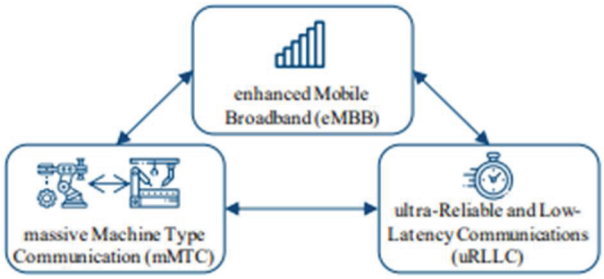

Figure 1 Three main characteristics of 5G-technology.

bandwidth, giving higher download speeds, eventually up to 10 gigabits per second (Gbit/s). In addition to 5G being faster than existing networks, 5G can connect more different devices, and even if people are in crowded areas, the servers will be more unified, improving the quality of Internet services [4].

2.1.1 Characteristic of 5G technology

The central characteristics of 5G communication relevant for the production industry sector and beyond are summarized by three services (Figure 1).

First, enhanced Mobile BroadBand (eMBB), with increased data rates above 1 Gb/s, reaching up to 20 Gb/s in downlink and 10 Gb/s in uplink [5].

Second, the massive Machine Type Communication (mMTC), aiming at large numbers of devices in wide areas [6]. Gupta et al. quantify it to 1,000,000 connections per km^2, while Aijaz et al. give the number of 100 nodes per m^2, so 100,000,000 per km^2. This scalability in terms of end nodes is the core aspect of mMTC. Energy-efficient operation (up to ten years battery live) for IoT devices keeps the large networks operational with little maintenance.

Third, ultra-Reliable Low Latency Communication (uRLLC), targeting symmetric up- and download latencies of 0.5 ms each way, summing up to the key figure of a 1 ms latency. The reliability reaches more than 99.999%. URLLC becomes fully standardized with the 3GPP Release 16, awaiting finalization in June 2020. Noteworthy is that in 1 ms, signals traveling at the speed of light can only cover a 100 km round trip distance, requiring edge cloud computing for the intended closed-loop control operations [7].

2.1.2 Architecture of 5G technology

The main goal of previous generations of mobile networks was simple: to provide fast and reliable mobile data services to network users. 5G has

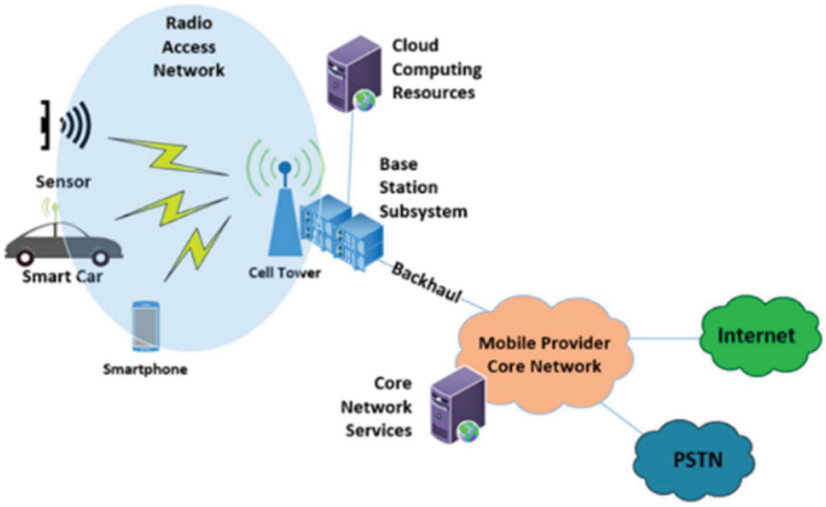

Figure 2 5G RAN system architecture.

extended this reach to offer a wide range of wireless services, delivered to the end user across multiple access platforms and over multi-layered networks.

5G is actually a dynamic, cohesive and flexible framework for multiple advanced technologies supporting a wide variety of applications. 5G uses a smarter architecture, with wireless access networks (RANs) that are no longer subject to the constraints of proximity to the base station or complex infrastructure. 5G is paving the way for a disaggregated, flexible and virtual wireless access network (RAN) with new interfaces creating additional data access points [8].

Take note that the RAN (see Figure 2) includes both the cell tower and the devices that are connected to the network. The cell tower, or base station, is referred to as the gNodeB (pronounced gee-node-bee), and the end-user devices are referred to as user equipment, or UE.

In addition to these components, the RAN includes baseband electronics found in both the base station subsystem (BSS), the user equipment (UE), transceivers, and the physical antennas themselves.

2.1.3 Security issues in 5G network

5G security is inherently prone to security vulnerabilities. Previous-generation networks relied on centralized hardware-based functions to provide security choke points that were relatively simple to monitor. Endpoints in distributed software-defined (SD) networks, such as 5G, are harder to

monitor. We can list below some security issues in technologies have an impact on 5G security [9].

Network vulnerabilities: SS7 and Diameter protocols were the mainstays of previous-generation networks. 5G employs standard internet protocols (IP) such as HTTP and TLS. These open-web protocols lower the entry barrier for both operators and hackers.

Decentralized security: With more routing points and devices, as well as faster speeds that benefit smash-and-grab attackers, security teams must rely more on automated monitoring and devise new methods to address the increased volume of security vulnerabilities.

Privacy and personal risk: The risk to 5G networks comes from a variety of devices, including seemingly innocuous home network appliances such as smart thermometers and intelligent thermometers, which may provide security chinks in network armor [10].

2.2 Vehicle to Everything

Vehicle to Everything (V2X) systems are a set of existing and future systems that enable vehicles to communicate with external entities. To be self-driving, a vehicle must be able to communicate with all the external elements that surround it and may influence its behaviour on the road [11].

According to the National Highway Traffic Safety Administration (NHTSA), implementing V2X technology will reduce traffic accidents in the United States. V2V (vehicle to vehicle), V2I (vehicle to infrastructure) [12] and V2N (vehicle to networks) are key components of V2X.

2.2.1 Vehicle to Vehicle technology

Vehicle to Vehicle (V2V) allows a vehicle to warn other vehicles of a potential danger or simply exchange information to keep traffic moving as smoothly as possible (see Figure 1). Vehicles can act and take measures to avoid a problem during a sudden change of trajectory or emergency based on the information exchanged, such as speed, location, direction of travel, braking, or even loss of stability.

V2V technology is actually a mesh network called VANET (Vehicular Ad-hoc Network) in which each vehicle corresponds to a node and is capable of transmitting, receiving and retransmitting information from other nodes [13]. This necessitates the installation of relay antennas, which are required for short-distance communication (300 meters) in a dense urban

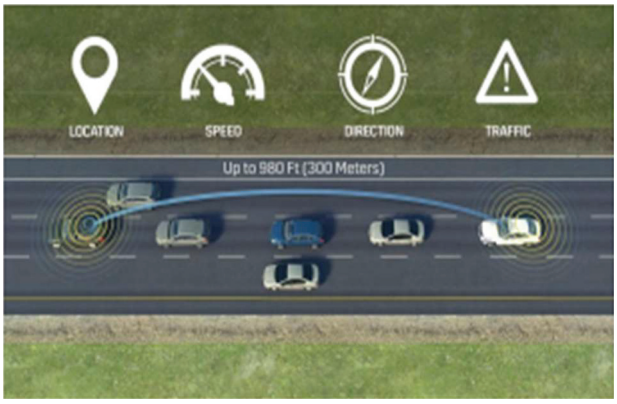

Figure 3 Communication between two vehicles.

environment saturated with waves. As a result, the United States Federal Communications Commission (FCC) has allocated a broad-spectrum frequency band ranging from 75 MHz to 5.9 GHz.

2.2.2 Vehicle to Infrastructure technology

Vehicle to Infrastructure technology (V2I) [14] is a communication technology that allows vehicles to communicate with the road infrastructures that surround them such as traffic lights, lane markers, lampposts, and parking, examples of infrastructure:

- Advanced Ground Markings: The pavement lane markings work with automated sensors to detect lines outside the visible wave spectrum, improving lane detection and traffic safety even in the most extreme weather conditions.
- Intelligent signage: We also need directional signage visible to humans and machines in all road conditions. Retro-reflective panels provide better readability, resulting in more precise navigation and faster decision making for drivers and automated vehicle systems.
- There is also a need for wireless communications to quickly identify construction areas and potential safety hazards so vehicle mobility and traffic can improve.

This communication is bidirectional and wireless. The data can be sent to vehicles via an ad hoc network and vice versa. An ad hoc network is a type of wireless network that is decentralized. This network does not rely on pre-existing infrastructure, such as routers or access points in wired networks.

Rather, each vehicle, participates in routing by relaying data to other nodes. V2I employs (DSRC) designed specifically for Intelligent Transportation Systems (ITS) [15]. It also employs another technology, Floating Car Data (FCD).

This data is primarily derived from terminals or applications on smartphones that are connected to the Internet. FCD data provides a better understanding and analysis of traffic conditions.

2.2.3 Vehicle to Network technology

Vehicle to Network (V2N) presents communication between a vehicle and equipment belonging to the cellular communication network, particularly Base Station (BS). These communications provide the functionality of V2I communications in areas not covered by roadside equipment (RSU). Thus, BS can be used to transmit information between vehicles: condition of the road, accident, etc. In addition, these V2N communications guarantee Internet access. Vehicles can therefore use them to connect to remote services. We can then speak of Vehicle-to-Cloud communications (V2C) [16]. These Cloud services may in particular correspond to global management applications of road safety or road traffic management.

2.2.4 Vehicle to Pedestrians technology

Vehicle to Pedestrians (V2P) is the communication between vehicle and pedestrians [17]. V2P systems are organized according to the different types of pedestrians found on the road. They have different characteristics:

- Individuals on foot (5 km/h). Each category has specific characteristics: children have unpredictable trajectories while the old people have slower trajectories.
- Cyclists (15 km/h). They circulate alone or in groups (the bikes are then generally placed in a straight line).
- Motorized two-wheelers (50 km/h). They generally travel alone.

The cell phone is the most commonly used tool in V2P systems allowing pedestrian communication due to its versatility and ubiquity. They are two modes of communication direct and indirect (or even hybrid). Direct modes of communication involve vehicles and pedestrians communicating directly between them [18]. Indirect modes of communication involve vehicles and UVCRs communicating with each other indirectly the direct mode of transmission implies that the vehicle and pedestrians are equipped with the same technology, which is not the case for the indirect mode of transmission.

V2P systems can use IEEE 802.11p technology, which has been specially designed for V2X communications, cellular technology (3G, C-V2X (5G)) or even Wi-Fi which cannot be used for large speed [19].

3 Cyber Security Issues

More specifically, to allow autonomous vehicles to communicate more easily with each other and with the outside world, frequency bands have been made available since 2008 (for example, the 5.9 GHz band for the ITS-G5 technology) to allow transmission of information relating to traffic conditions and the road environment. In March 2018, the PSA Group and Qualcomm Technologies, partners since February 2017, carried out a first C-V2X demonstration in France. Volkswagen began rolling out new vehicles in 2019 that work with ITS-G5 technology (explained later). As for the C-V2X, a less mature and more recent technology than the previous one, the PSA and Ford groups have plans for 2020 in the United States. ITS-G5 technology is therefore, and has been since 2019, the solution used while waiting for the arrival of new technologies such as C-V2X. Regarding the latter, it uses 5G, and it is since the beginning of 2017 that several applications have been tested, marking an important step in the deployment of 5G for connected vehicles.

The 5G architecture contains two major parts: New Generation Radio Access Network (NG-RAN) and a 5G Core (5GC) network (see Figure 4). The first one includes the new Generation Node Base (gNB) station that connect vehicles with the core network. For the 5G network core is based on the breakdown of the control plane and the user plane, it consists of different entities such as access and mobility management function (AMF), security anchor function (SEAF), authentication server function (AUSF), authentication credential repository and processing function (ARPF), and unified data management (UDM) [20]. AMF is responsible for handling connection and mobility management tasks. SEAF is used for authentication and communication. AUSF performs identity verification. ARPF calculates authentication data and keys. UDM carries functions related to data management.

To sum up, the numerous tests underway on the C-V2X technology have made it possible to plan the first commercial launch for 2020 in the Chinese market.

Future vehicles will be equipped with new means of processing, communication and sensor technologies, and new generations of human/machine

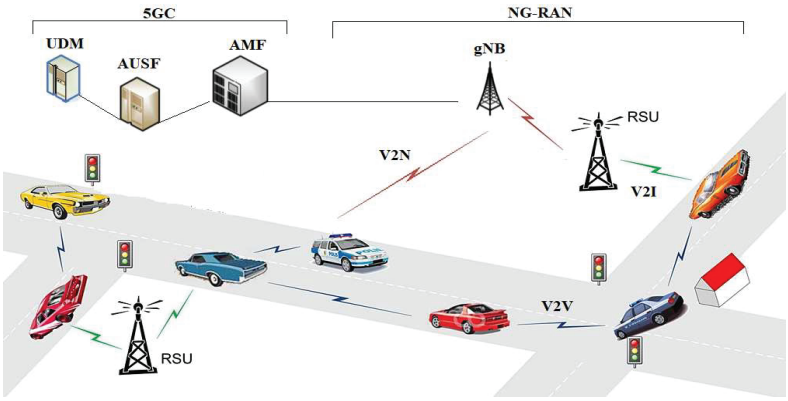

Figure 4 System model.

interfaces. This will require guaranteeing the security aspect in V2Xs, such as

- Securing of information received and transmitted by vehicles by making them anonymous.
- Integration of advanced and automatically updated systems capable of detecting any sort of intrusion.
- Securing the car's wireless technologies (Wi-Fi and Bluetooth in particular).

3.1 Safety Requirements for 5G Based V2X Applications

The characteristics of V2X applications impose specific safety requirements. These requirements are listed below:

Authentication and Authorization: Authentication and authorization must be provided to allow only trusted entities to participate in the V2X communication system. This authentication and authorization can be revoked to exclude malicious entities from the C-ITS system.

Data integrity: Security mechanisms must ensure that the data sent is not manipulated by malicious entities

Confidentiality: Confidentiality may be required by some V2X applications. The content of sent messages must be confidential

Privacy protection: privacy protection mechanisms must be put in place to avoid tracking vehicles or making the link between their temporary identities by malicious entities internal or external to the C-ITS communication system.

3.2 Security Solutions for 5G Based V2X

Autonomous Car Security: Autonomous vehicles rely on real-time data and instructions from various sensors linked to a cellular network. The V2X communications allow access to the guidance maps for real-time coordination. The security features of V2X help in the prevention of impersonation and replay attacks, which could misdirect the vehicle and cause interruptions and accidents.

Driver Authentications: In assisted vehicles, secure V2X operations can help in the verification of drivers through third-party authentications. The driver's medical conditions can also be verified using attached sensors, and several lightweight authentications can help in quantifying access control to the legitimate driver.

Vehicle-Health Monitoring: The vehicle's health can be monitored using V2X, which sends real-time instructions to car software maintainers for every machine issue. During wrong-configurations, an intruder has a high chance of gaining access to vehicle components, which can then be used to gain access to the entire network. In V2X, such situations can be encountered by establishing a secure communication channel.

Anomaly Detection and Traffic Management: Traffic management includes issues such as speed management, traffic information, routing information, cooperative navigation, and so on [21]. Furthermore, driver behaviour, vehicular anomalies, and network intruders all have an impact on the core functionalities of the vehicular system. Sufficiently secure mechanisms can aid in the resolution of these issues and the detection of potential anomalies prior to their attack.

4 Related Work

The future Intelligent Transportation System (ITS) is highly dependent on the Vehicle-to-Everything (V2X) communication system, which is an important and significant component of its system. Furthermore, the European Telecommunications Standards Institute (ETSI) has established Intelligent Transport Systems (ITS) or vehicle-to-everything (V2X) communications standards. The main goal of V2X is to improve traffic management, a stack of protocols, procedures for security and road safety [22]. V2X communications refer to a vehicle's information sharing with other ITS components such as pedestrians,

other vehicles, transportation infrastructure (e.g., traffic signs and lights), and Internet gateways [23].

The automotive industry has seen a revolutionary change in the last decade, with vehicles context awareness, networking, communication, and data processing capabilities to enhance user experience, encourage traffic safety, and prepare the way for the realization of automated driving. The vision of linked automobiles, in which vehicles loaded with communication modules are networked with their local surrounds and beyond, has now become a popular reality. After smart phones and tablets, linked cars have become one of the fastest-growing categories of connected device [24,25]. As a result of the large number of vehicles connected to the Internet of Things (IoT), conventional Vehicle Adhoc Networks (VANETs) are being built for the Internet of Vehicles (IoV) [23]. Vehicles and roadside equipment are regarded as connecting nodes in vehicular cellular networks. These connecting nodes exchange data sets such as speed, orientations, current position, traffic conditions, unexpected braking, and safety alerts. Vehicle-to-Vehicle (V2V) communications refer to connections between vehicles, whereas Vehicle-to-Infrastructure (V2I) communications refer to connections among both vehicles and infrastructure node(s) [26]. Both V2V and V2I have received increased attention as a promising benefit in terms of safe driving, congestion control, and traffic effectiveness. More clearly, Vehicle applications and communications technologies are generally known to as vehicle to everything (V2X), which is broadly classified into four distinct types: vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to network (V2N), and vehicle to pedestrian (V2P). Moreover, according to studies, Vehicle-to-Everything (V2X) will decrease 80 percent of existing road traffic accidents and contribute to the implementation of a better, and safer public transportation system [27–30]. Furthermore, V2X might provide multimedia services, which provide customers with greater and entertaining [31].

The concept of V2X communication is a critical component of vehicular communication technology. Various communication systems are available, including Wi-Fi, WiMAX, Long Term Evolution (LTE), and DSRC, although not all of them can provide the least delay, dependability, and accuracy required for collision avoidance in connected vehicles. For instance, the DSRC technology provides some benefits such as speedy network access, limited communication latency, and extremely robust security communication for numerous protection applications; nevertheless, relying only on DSRC is not a good solution for diverse connected vehicle systems [32]. However, according to statistical data acquired from [33], road accidents in

Europe in 2014 resulted in the deaths of around 25,700 individuals and the injuries of another 200,000. As a result, V2X is being implemented through the platforms ERTICO [34] and Cooperative-ITS. The European Commission also proclaimed an ambitious objective of reducing the number of fatalities on European roads by half by 2020. As a result, integrating the communication technologies required for autonomous driving will provide critical assistance for the establishment of new security standards. In the United States, General Motors has completed the signing of vehicles equipped with V2X technology. Furthermore, four states in the United States (Nevada, Florida, California, and Columbia) have previously enacted legislation allowing the use of motor vehicles on public roadways. Moreover, countries in Asia are developing smart transportation systems based on V2X such as road transport administration is constructing an ITS environment dedicated to V2X technology and development in Singapore [35]. Toyota Motor Corp. and KDDI Corp. of Japan took the lead in developing a worldwide communication network for the marketing of linked automobiles [36]. Tongji University and The National Intelligent Connected Vehicle Pilot Zone in China are conducting research on 25 self-driving automobiles made up of devices, transmission units, and other sensors [37].

Thus, Visiongain's study [38] in 2016 illustrates the rising relevance of V2X in vehicle communication. Focusing on complete research of the V2X worldwide market, the report's findings show that V2X is rapidly advancing in today's auto sector. According to Visiongain's findings, the V2X sector has the potential to generate over than 37 billion dollars in revenue and sell 47.1 million vehicles equipped with V2X modules. Several parties are paying close attention to the application of V2X in the automotive industries. Vehicular networks, on the other hand, should not be confused with regular cellular networks. V2X communication, for instance, necessitates networks that offers superior portability, availability, and reduced latency. Consequently, several technologies, including ZigBee, Bluetooth, Dynamic Short-Range Communication (DSRC), WiFi Direct, and others, were unable to satisfy these requirements [39]. Network nodes, particularly 5G, are regarded as one of the finest choices for implementing vehicle networks. 5G can allow high transportation while also providing a vast service area and high strain rates. They also have an authorized band [40].

IoT technology is critical for linking physical things and working collaboratively via the Internet [41]. Furthermore, the Internet of Vehicles (IoV) is being established expressly to link vehicles via the Internet, allowing them to acquire and transmit data, as well as for monitoring and localisation [42–44].

Fifth Generation (5G) systems are defined as being completely versatile, with configurable end-to-end communication, processing infrastructures, and networking [45]. All of these aspects contribute to improved results in terms of speed, dependability, scalability, delay, and availability, along with meeting the varied needs of numerous services. 5G systems are projected to aid in the development of new services needed by developing and significant fields such as V2X. The 5G capability needs necessitate increased spectrum performance, which encourages study into interference control for device-to-device communication. Regardless of the particular quality standards, the diversity of the services, transport networks, and devices that 5G must serve will undoubtedly need considerable changes to the network infrastructure. To deal with such diversity, adaptability will be a crucial feature of the next networks [46]. The authors of this study [47] describes a revolutionary FANET routing protocol based on a modified AntHocNet to stabilize parameter enhances energy quality and operational system performance.

Authors of one such paper [48] presented a general system defining network service infrastructure based on a similar main network and multiple RANs, as well as a mobile phone network Software Defined Network (SDN) controller. The scripting capability of RANs increases their possibilities, and the rail infrastructure is made up of configurable networking equipment. The authors recommended two techniques. The authors used an SDN controller to create the prescribed application in the first approach. The Control Plane (C-Plane) operations are explicitly written into the SDN controller in the second technique. The authors of [49] created a 5G system that consists of two different networks (L1 and L2), a radio network, and a network cloud. The radio network offers the minimal amount of L1 and L2 functionality, whereas the network cloud is in charge of higher layer functionality. This system effectively yields a network protocol by merging the Access Stratum (AS) and Non-access Stratum (NAS) features. To accomplish changing network installation, the RAN L2 and gateway capabilities in the CN are unified on the access network. Some other paper [50] relies on a 5G C-Plane capable of providing connection monitoring as a utility while still supporting portability, handovers, and traffic monitoring. The RAN and CN functionalities are combined and executed as separate apps with one or many multilayer devices. The authors of [51] propose latest systems like mmWave and VVLC that will be included into the 5G V2X access infrastructure to enable specific V2X application. The proposed cmWave macro-cellular system is planned to operate with LTE-based communication network as well as IEEE 802.11p. The macro-cellular network will provide enhanced availability, large data

speeds, and reduced latency for control information. The macro-cellular system will also be linked to smaller units, RSUs, and other infrastructure components. The technological advances would be enabled to provide quick high transmission, which would be an essential component of the future 5G V2X network system.

Thus, with the expansion of V2X communications under 5G systems, further utilization for V2X applications outside road traffic management effectiveness are anticipated, including rostering, expanded monitoring, enhanced mobility, online trying to drive, and others [52]. These sophisticated technologies are projected to have even more strict delay (tenths of milliseconds), robust approach dependability (up to 100 percent), and higher communication area needs, all of which may be met by 5G systems.

5 Proposed Scheme

In this paper, we propose a 5G based V2X communication security model, which consists to ensure reliable and secure authentication between vehicles, Infrastructure and 5G network.

5.1 Vehicle to Infrastructure

In this case, each vehicle is authenticated with RSU without a trusted third-party authority. We consider an ECDH algorithm to ensure vehicle authentication via RSU and the digital signature algorithm based on attributes to sign the messages by vehicles. The aim to use elliptic curves and attributes algorithms is their faster processing compared to others cryptographic methods.

The Figure 5 illustrates the procedure of authentication and communication between vehicle and RSU. Still, the description in detail of all steps is as follows:

- The vehicle Vi and RSU choose together an elliptical curve E (a, b, K) and a point P on the curve
- Vi secretly chooses kVi and calculates kVi.P
- RSU secretly chooses kRSU and calculates kRSU.P
- Vi and RSU calculate the shared secret Ss=kVi.kRSU.P
- The authentication of the vehicle by the RSU is ensured by the ABS signature process using the private key KPR and the ABS verification using the public key KPUB.

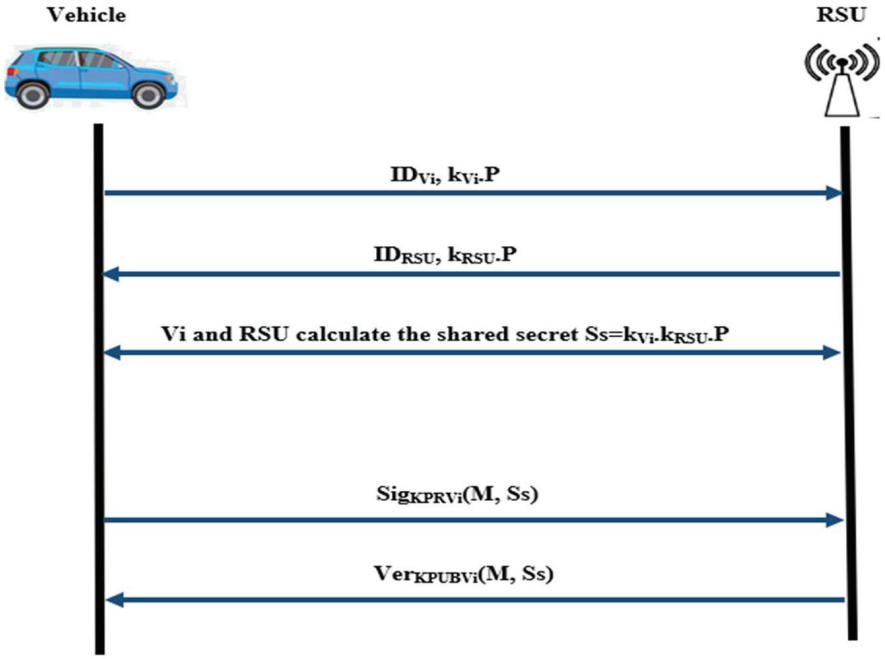

Figure 5 Authentication and communication between vehicle and RSU.

Figure 6 Communication between vehicles.

With KPRVi is kVi KPUBVi is E (a, b, K), P and kVi

KPRRSU is kRSU KPUBRSU is E (a, b, K), P and kRSU

For data transmission between vehicles, we use elliptical curve encryption algorithm to guarantee that the message authentication is establish with success as shown in Figure 6.

5.2 Vehicle to Network

In vehicle to network communication, we suggest to improve an authentication and key agreements protocol for 5G network to overcome standard authentication protocol 5G-AKA limitation [53]. Our proposed protocol pursues 5G cellular network architecture and resists many threats including

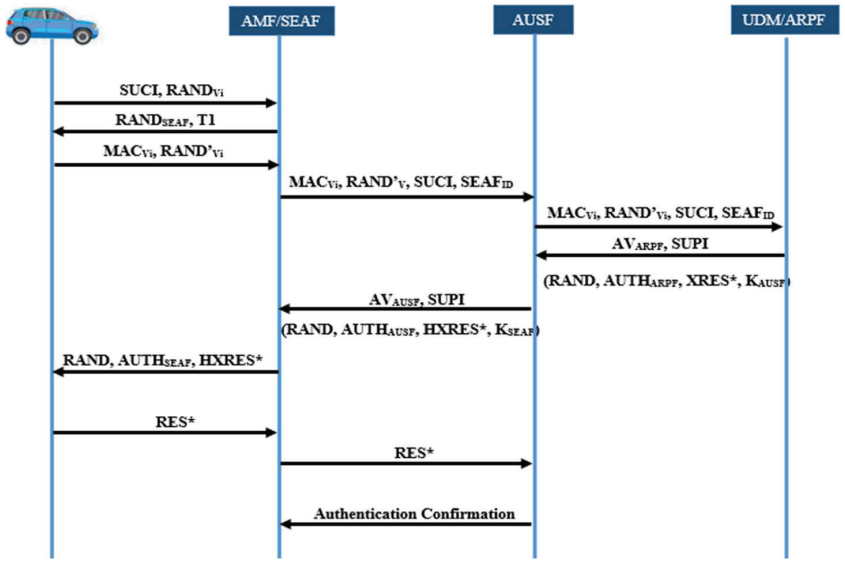

Figure 7 Improved 5G-AKA for V2N communication.

replay attack, redirection attack, man in the middle attack and DoS attack (Figure 7).

Actually, in our proposal, the authentication process and key agreements are established between vehicles, AMF/SEAF, AUSF, and UDM/ARPF. Each vehicle has a permanent identity called SUPI that the provider has to install which permits the user to register in the 3GPP core network. We regard the Elliptical Curve Diffie Hellman Key Agreement protocol, which provides for the establishment of a shared secret key via an unsecured channel, and utilize symmetric encryption in order to encrypt the identity, for the purpose of obtaining a Subscription Concealed Identifier (SUCI) that hidden the SUPI calculated by the UE.

In addition, we assume that communication between core network entities and security functions (AMF/AUSF/ARPF) is secure, and long-term IPSec, (D) TLS, or DIAMETER sessions are maintained across established channels between identified entities.

6 Validation and Evaluation

In this section, we analyse the formal verification of our model and we evaluate the performance in terms of operational cost.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/proposed_Scheme.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 1 states
  Translation: 0.09 seconds
  Computation: 0.00 seconds
```

Figure 8 OFMC Back-End results report.

6.1 Security Analysis

Our scheme was verified by a tool of security verification, Automated Validation of Internet Security Protocols and Applications (AVISPA) [54] which supports automatic and rigorous validation of internet security protocols. The main principle of our model is to assure security requirements such as mutual authentication, integrity, confidentiality between the vehicles, RSU and the equipment of 5GC network (SEAF, AUSF and ARPF).

In fact, Figures 8 and 9 present the specification of our model using two backends OFMC and CLAtSe respectively, according to these figures we can conclude that our solution achieves the goal of security and can overcome many malicious attacks.

6.2 Operational Cost

To evaluate the performance of our system in terms of operational cost, we choose to implement the execution time values of all cryptographic algorithms and operations considering our solution and other existing ones using Crypto++ Library [55] running on a test platform with 2.1 GHz processor using Ubuntu. Table 1 shows that our used operations are faster and more efficient.

Figure 9 CL-AtSe back-end results report.

Table 1 Execution time of algorithms/protocols

Operations	Algorithms/Protocols	Execution Time (μs)
Key Exchange	DH	2
	ECDH	1.29
Digital Signature	DSA	2.47
	ECDSA	5.38
	ABS	1.2
Asymmetric Encryption	RSA	6.28
	El-Gamal	5.97
	ECC	4.33

7 Conclusion

The deployment of vehicular communication networks today appears to be a relevant solution to ensure the safety of road users and make road traffic more fluid. In an effort to improve road safety, vehicles are becoming increasingly intelligent and able to detect potentially dangerous obstacles. It is therefore necessary to share information between vehicles (V2V) on the one hand and between vehicles and infrastructure (V2I) and (V2N) on the other hand. Among the problems that have arisen in these networks is the problem of authentication and confidentiality of data transmitted between entities. Our

scheme allows vehicles to establish secret key and authenticate in RSU in a reliable way using digital signature by ABS algorithm and also secure the communication between vehicles using the cryptographic keys obtained in the phase of key exchange by ECDH. In addition, our proposed consist to improve an authentication and key agreement protocol for 5G network to ensure security and overcome the limitations of existing 5G-AKA in V2N communication.

In future research work, we aim to create a simulation analysis of our Lightweight and Secure Authentication Model in a real vehicular environment such as in urban and highway scenarios.

References

[1] G. Dimitrakopoulos, P. Demestichas, 'Intelligent transportation systems'. IEEE Vehicular Technology Magazine, 5(1), 77–84, 2010.

[2] J. Wang, Y. Shao, Y. Ge, R. Yu, 'A survey of vehicle to everything (V2X) testing'. Sensors, 19(2), 334, 2019.

[3] N. E. El Faouzi, H. Leung, A. Kurian, 'Data fusion in intelligent transportation systems: Progress and challenges–A survey'. Information Fusion, 12(1), 4–10, 2011.

[4] Kim, Dongwook, and Sungbum Kim. 'Network slicing as enablers for 5G services: state of the art and challenges for mobile industry.' Telecommunication Systems 71.3, 517–527, 2019.

[5] Settembre, Marina. 'A 5G Core Network Challenge: Combining Flexibility and Security'. In: 2021 AEIT International Annual Conference (AEIT). IEEE. pp. 1–6, 2021.

[6] Rodriguez, Veronica Quintuna, Fabrice Guillemin, and Amina Boubendir. 'Automating the deployment of 5G network slices using ONAP,' 10th International Conference on Networks of the Future (NoF). IEEE, 2019.

[7] Idowu-Bismark, Olabode, et al. '5G Small Cell Backhaul: A Solution Based on GSM-Aided Hybrid Beamforming.' IJ Computer Network and Information Security, 24–31, 2019.

[8] Forge, Simon, and Khuong Vu. 'Forming a 5G strategy for developing countries: A note for policy makers. ' Telecommunications Policy, 101975.2019, 2020

[9] Sohaib, Rana Muhammad, et al. 'Network Slicing for Beyond 5G Systems: An Overview of the Smart Port Use Case.' Electronics, 2019.

[10] Shaik, Altaf, Borgaonkar, Ravishankar, Park, Shinjo, et al. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 221–231, 2019.

[11] R. Molina-Masegosa, J. Gozalvez, M. Sepulcre, 'Comparison of IEEE 802.11 p and LTE-V2X: An evaluation with periodic and aperiodic messages of constant and variable size'. IEEE Access, 8, 121526–121548

[12] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, J. Martin, 'Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation'. Transportation Research Part C: Emerging Technologies, 68, 168–184, 2016.

[13] Y. Ota, H. Taniguchi, T. Nakajima, K. M. Liyanage, J. Baba, A. Yokoyama, 'Autonomous distributed V2G (vehicle-to-grid) satisfying scheduled charging'. IEEE Transactions on Smart Grid, 3(1), 559–564, 2011.

[14] M. Bagheri, M. Siekkinen, J. K. Nurminen, 'Cellular-based vehicle to pedestrian (V2P) adaptive communication for collision avoidance'. In 2014 international conference on connected vehicles and expo (ICCVE) (pp. 450–456). IEEE, 2014.

[15] A. Ghosal, M. Conti, 'Security issues and challenges in V2X: A survey'. Computer Networks, 169, 107093, 2020.

[16] L. Mendiboure, 'Distribution géographique de données dans l'Internet des Véhicules: une approche logicielle et sécurisée utilisant les réseaux cellulaires', Doctoral dissertation, Université de Bordeaux, 2020.

[17] J. Zhang, F. Y. Wang, K. Wang, W. H. Lin, X. Xu, C. Chen, 'Data-driven intelligent transportation systems: A survey'. IEEE Transactions on Intelligent Transportation Systems, 12(4), 1624–1639, 2011.

[18] S. A. A. Hakeem, A. A. Hady, H. Kim, 'Current and future developments to improve 5G-NewRadio performance in vehicle-to-everything communications'. Telecommunication Systems, 75(3), 331–353, 2020.

[19] S. Laqtib, K. El Yassini, M. L. Hasnaoui, 'A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET'. International Journal of Electrical and Computer Engineering, 10(3), 2701, 2020.

[20] M. Ouaissa, M. Houmer, M. Ouaissa, 'An enhanced authentication protocol based group for vehicular communications over 5G networks'. In 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1–8). IEEE, 2020.

[21] S. Laqtib, K. El Yassini, M. L. Hasnaoui, 'A novel energy aware OLSR in mobile ad hoc networks: EA-OLSR'. In International Conference on Research in Applied Mathematics and Computer Science (Vol. 2021). ICRAMCS 2021, 2021.
[22] S. Arslan, M. Saritas, 'The effects of OFDM design parameters on the V2X communication performance: A survey'. Vehicular Communications, 7, 1–6, 2017.
[23] K. Abboud, H. A. Omar, W. Zhuang, 'Interworking of DSRC and cellular network technologies for V2X communications: A survey'. IEEE transactions on vehicular technology, 65(12), 9457–9470, 2016.
[24] W. Sun, D. Yuan, E. G. Ström, F. Brännström, 'Cluster-based radio resource management for D2D-supported safety-critical V2X communications'. IEEE Transactions on Wireless Communications, 15(4), 2756–2769, 2015.
[25] R. P. Jover, 'Security and impact of the IoT on LTE mobile networks'. Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations, 6, 2015.
[26] M. T. Kawser, M. S. Fahad, S. Ahmed, S. S. Sajjad, H. A. Rafi, 'The perspective of vehicle-to-everything (v2x) communication towards 5g'. IJCSNS, 19(4), 146, 2019.
[27] H. T. Cheng, H. Shan, W. Zhuang, 'Infotainment and road safety service support in vehicular networking: From a communication perspective'. Mechanical systems and signal processing, 25(6), 2020–2038.
[28] CAMP Vehicle Safety Communications Consortium. 'Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by DSRC'. National Highway Traffic Safety Administration, US Department of Transportation, Washington DC (2005).
[29] C. Bila, F. Sivrikaya, M. A. Khan, S. Albayrak, S. 'Vehicles of the future: A survey of research on safety issues'. IEEE Transactions on Intelligent Transportation Systems, 18(5), 1046–1065, 2016.
[30] R. Baldessari, B. Bödekker, M. Deegener, A. Festag, W. Franz, C. C. Kellum, W. Zhang, 'Car-2-car communication consortium-manifesto'.
[31] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, M. Guizani, 'Heterogeneous information network-based content caching in the internet of vehicles'. IEEE Transactions on Vehicular Technology, 68(10), 10216–10226, 2019.
[32] N. A. N. Ch, 'Intelligent traffic monitoring and control system'. University of Alaska Fairbanks, 2019.

[33] European Commission. (2015). Road safety in the European Union: Trends, statistics and main challenges. Technical Report.

[34] Ertico, Together we bring intelligence into mobility, 2018, (Accessed on October 15). [Online]: http://ertico.com.

[35] NTU Media Release, Paving the way for Singapore's future land transport system, 2018, (Accessed on October 12). [Online]: http://media.ntu.edu.sg/NewsReleases/Pages/newsdetail.aspx?news=d0466790-8dc3-47c2-854b-e1c15efc02b1.

[36] KDDI, Toyota and kddi to jointly promote establishment of global communications platform to support car connectivity, 2018, (Accessed on October 12). [Online]: https://global.kddi.com/company/news/detail/toyota-and-kddi-global-communications-platform-to-support-car-connectivity.html.

[37] Shanghaidaily, Autonomous connected cars on their way, 2018, (Accessed on October 12). [Online]: http://www.shanghaidaily.com/business/biz-special/Autonomous-connected-cars-on-their-way/shdaily.shtml.

[38] A. Alnasser, H. Sun, J. Jiang, Cyber security challenges and solutions for V2X communications: A survey. Computer Networks, 151, 52–67, 2019.

[39] Hussein, H. H., Elsayed, H. A., El-kader, A., & Sherine, M. (2020). Intensive Benchmarking of D2D communication over 5G cellular networks: prototype, integrated features, challenges, and main applications. Wireless Networks, 26(5), 3183–3202.

[40] Salem, M. A., Tarrad, I. F., Youssef, M. I., & Abd El-kader, S. M. (2020). An adaptive EDCA selfishness-aware scheme for dense WLANs in 5G networks. IEEE Access, 8, 47034–47046.

[41] Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. Engineering, 3(5), 616–630.

[42] P. M. Kumar, G. Manogaran, R. Sundarasekar, N. Chilamkurti, R. Varatharajan, 'Ant colony optimization algorithm with internet of vehicles for intelligent traffic control system'. Computer Networks, 144, 154–162, 2018.

[43] A. Tolba, 'Content accessibility preference approach for improving service optimality in internet of vehicles'. Computer Networks, 152, 78–86, 2019.

[44] G. A. Akpakwu, B. J. Silva, G. P. Hancke, A. M. Abu-Mahfouz, 'A survey on 5G networks for the Internet of Things: Communication technologies and challenges'. IEEE access, 6, 3619–3647, 2017.
[45] 3GPP, Feasibility Study on New Services and Markets Technology Enablers, Stage 1, Technical Report, Technical Specification Group Services and System Aspects, 2016.
.
[46] NGMN, Next Generation Mobile Networks, Technical Report, NGMN Alliance, 2015.
[47] Khan, I. U., Qureshi, I. M., Aziz, M. A., Cheema, T. A., & Shah, S. B. H. (2020). Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). IEEE Access, 8, 56371–56378.
[48] C. Bernardos, A. De La Oliva, P. Serrano, An architecture for software defined wireless networking, IEEE Wirel. Commun. 21 (3) 52–61, 2014.
[49] P. Agyapong, M. Iwamura, K.W. Staehle D, A. Benjebbour, Design considera- tions for a 5g network architecture, IEEE Commun. Mag. 65–75, 2014
[50] V. Yazici, U. Kozat, M. Sunay, A new control plane for 5g network architecture with a case study on unified handoff, mobility, and routing management, IEEE Commun. Mag. 76–85, 2014.
[51] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger, W. Xu, Use cases, require- ments, and design considerations for 5g v2x, arXiv: 1712.01754, 2017.
[52] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, L. Zhao, Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G, IEEE Commun. Stand. Mag. 1(2) 70–76, 2017.
[53] M. Ouaissa, M. Ouaissa, 'An Improved Privacy Authentication Protocol for 5G Mobile Networks'. In 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM) (pp. 136–143). IEEE, 2020.
[54] AVISPA Project: http://www.avispa-project.org/
[55] Crypto++ Library: http://www.cryptopp.com/

Biographies

Meriem Houmer received the bachelor's degree in System and networks from Chouaib Doukkali University in 2013, the master's degree in information system, network and multimedia from Sidi Mohamed Ben Abdellah University in 2015, and the philosophy of doctorate degree in computer science and networks from Moulay Ismail University in 2021, respectively. She is currently working as an Assistant Professor at Higher school of technologies, Ibn Zohr University, Dakhla, Morocco. Her research areas include routing protocols and security in vehicular ad hoc and 5G networks.

Safaa Laqtib received a Master's degree in multimedia and decision-making computer systems from the Faculty of Science Dhar El Mahraz FSDM, in 2013 and 2015, respectively. Currently, she obtained a doctorate in Computer Science from the Faculty of Science Meknes. Her current research interests include mobile ad hoc networks, deep learning, machine learning, and wireless sensor networks, vehicular ad hoc networks, Cybersecurity of mobile ad hoc networks.

Siham Eddamiri is a Researcher Associate in Computer Science at the National Higher School of Arts and Crafts (ENSAM), Moulay Ismail University (UMI), Meknes, Morocco. She is a member of the research Laboratory LM2I funded by the Industrial Engineering and Productivity Department (ENSAM). Her research focus is on the domain of white-box machine learning for critical domains and (semantic) knowledge models. Other research interests are bio-inspired algorithms and extracted knowledge from the RDF dataset in general.