computers

MDPI

Review

Cybersecurity in Intelligent Transportation Systems

Teodora Mecheva and Nikolay Kakanakov *

Plovdiv Branch, Technical University of Sofia, 4000 Plovdiv, Bulgaria; teodora.mecheva@tu-plovdiv.bg
* Correspondence: kakanak@tu-plovdiv.bg; Tel.: +359-895-587-568

Received: 31 August 2020; Accepted: 6 October 2020; Published: 13 October 2020

Abstract: Intelligent Transportation Systems (ITS) are emerging field characterized by complex data model, dynamics and strict time requirements. Ensuring cybersecurity in ITS is a complex task on which the safety and efficiency of transportation depends. The imposition of standards for a comprehensive architecture, as well as specific security standards, is one of the key steps in the evolution of ITS. The article examines the general outlines of the ITS architecture and security issues. The main focus of security approaches is: configuration and initialization of the devices during manufacturing at perception layer; anonymous authentication of nodes in VANET at network layer; defense of fog-based structures at support layer and description and standardization of the complex model of data and metadata and defense of systems, based on AI at application layer. The article oversees some conventional methods as network segmentation and cryptography that should be adapted in order to be applied in ITS cybersecurity. The focus is on innovative approaches that have recently been trying to find their place in ITS security strategies. These approaches includes blockchain, bloom filter, fog computing, artificial intelligence, game theory and ontologies. In conclusion, a correlation is made between the commented methods, the problems they solve and the architectural layers in which they are applied.

Keywords: ITS; IoT; VANET; cybersecurity

1. Introduction

Internet of things (IoT) is a consequence of converging of several technologies like: real-time analytics, machine learning, embedded systems, wireless networks, control systems, home and building automation. From the consumer point of view, IoT is a synonymous to products pertaining to the concept of the intelligent home, intelligent healthcare, intelligent city and so forth. Many of these areas have similar characteristics and face similar challenges. Borrowing technologies between IoT sub-areas is common but needs to be considered well and explored in practice. Despite the similarities, even within the same area the requirements for communication range and bit rate, real-time operation, reliability and security vary. As sub-area of the smart city Intelligent Transportation Systems (ITS) are characterized by many of the features of IoT. Their distinctive features are: strict time requirements, dynamics and large volumes of data. One of the main characteristic property of the ITS is the high demand of cybersecurity. ITS applications can be classified as: transport safety, road traffic efficiency and infotainment. Road safety applications have very high cybersecurity requirements combined with hard real time constrains. Although road traffic efficiency and infotainment applications are not directly related to the physical safety of road users, cybersecurity requirements remain high, as a breach in any of them can reflect on the efficiency of the whole ITS. For example, overloading the communication channel for infotainment application purposes may interfere with the normal operation of security application, which may be critical [1].

Vehicular ad-hoc networks (VANET) are a key component of all modern developments for ITS. Nodes (vehicles) in VANET exchange short messages, called beacons, during certain periods.

The beacons contain important information about vehicles and the environment, for example, direction, acceleration, speed, road conditions, weather conditions and so forth. Connecting vehicles in wireless one hop communication poses many tasks such as authentication of newly joined vehicles, the need to protect the identity of the user, interruptions, providing multi hop communication, high heterogeneity (depending on whether the cars are congested in a big city or in a suburban area). Much of the research on ITS cybersecurity focuses on network security [2–5].

Reference [6] indicates the importance to maintain connectivity of nodes with software-configurable security services that ensure protection. This need is dictated by the characteristics of VANET—high dynamics in changes of network topology, uncertain structure, unclear network perimeter, high mobility, enabling and disabling of nodes.

Reference [7] compares the two main technologies for VANET—cellular and based on Wi-Fi. It points out that knowing the strengths and weaknesses of each technology is a step towards stable and secure communication in VANET.

In Reference [3] the authors emphasize the need of an efficient and secure authentication and privacy scheme and offer storage a group of aliases through a bloom filter. The experiment will be discussed in more detail in Section 5.

VANETs are not the only vulnerable component of ITS. Cybersecurity in a system as complex as ITS takes place on all levels. Efforts to automate transport have led to the application of Fog and Cloud computing, artificial intelligence and machine learning in ITS. This can significantly slow down the actual application of fully automated vehicles due to the complexity of ensuring cybersecurity. The non-technological aspect of ITS security should not be underestimated. It is expressed in careful consideration of authorization policy, development of standards, governance, policy, regulation, awareness and education [8].

In Reference [9] the authors overview the main ITS enabling technologies—smart vehicles, public transportation, IoT devices, networking and summarizes the issues by linking them to the relevant components in ITS. The authors argue that the most outstanding advantage of removing the human factor during the driving task is that traffic safety will be improved. In order to achieve that a cybersecurity strategy should be established. The authors highlight the role of the politics and the necessity of international benchmarked regulatory framework.

Reference [10] emphasize the connection between Connected Automated Vehicles (CAVs) and road safety. The authors consider that standardization of procedures, education of the society and establishing dedicated communication networks for additional security between communicating vehicles are important ways to implement cybersecurity in CAV.

In Reference [11] the focus is on certifications and audits based on standards and regulations developed in cybersecurity for CAVs. The main difficulty is the complexity of the system combining robotic vehicles and vehicles driven by humans, pedestrians, cyclists and so forth. Another aspect is social IoT enabling Mobility as a service (MaaS). There are significant unanswered questions concerning privacy and the reliability of the information. The answers to these questions will largely determine what ITS will look like in the future. The authors believe that a very restrictive regulation will slow down CAVs development and real-world deployment but this is a necessity to prevent safety and security from being sacrificed by commercial interests.

2. ITS Cyberattacks

The heterogeneity of ITS complicates the task of classifying and identifying cyberattacks. This section lists ITS specific attacks, which will later be associated with the architectural layers:

2.1. VANET Man-in-the-Middle Attack

The man-in-the-middle attack is a classic type of cyberattack, that the attacking party intercepts messages between the two communicating parties and forwards modified content. In case of man-in-the-middle attack on the physical and data link level in VANET, the attacking party take into

account the fact that the nodes have a certain range. They either have to attenuate the signal or they have to modify the location information in case they take advantage of a situation where the attacked nodes are out of range but the attacking party is in the range of both nodes. Example of man-in-the middle VANET attack: the attacking party interferes in the communication between two or more vehicles and changes their location information. This can disrupt the proper functioning of road safety or efficient traffic applications [9,12].

2.2. Routing Attacks

The physical and the data link level of VANET define one-hop communication. Multi-hop communication is provided by routing protocols. Routing attacks are cases in which there is a breach in the routing protocols of VANET and a malicious node prevents the data from reaching their final destination. Black hole attack is an example of a routing attack in which, malicious node silently drops all the packets, that are supposed to be re-transmitted. Gray hole attack is another sub-type of routing attack in which dropping is performed only on selective packets [9,12].

2.3. Timing Attacks

Timing attacks cause a communication delay and thus disrupts the operation of applications that have real-time requirements. For example, in a cooperative adaptive cruise control system an emergency message is sent to the neighboring vehicle in order to prevent collision. If the attacking party manages to cause a delay (for instance by overloading the network traffic), despite the correct receipt of the data, the reaction in the braking system will delay and the collision will not be prevented [12].

2.4. Spoofing

In case of spoofing attack the attacking party broadcast corrupt data in order to cause invalid reaction in the system. Example: The attacking party is sending bogus GPS coordinates and thus disrupting the operation of the navigation system [9].

2.5. Denial-of-Service Attacks (DoS)

DoS is a classic cyberattack that affects the availability of system components. In ITS it is especially dangerous in case some safety critical feature is concerned. Sybil is typical VANET DoS attack in which a malicious vehicle impersonates as multiple identities and injects false broadcast messages into the network. Thus disrupts the normal exchange of information [9,12].

2.6. Internal Vehicle Network Attack

Due to the fact that most internal vehicle networks are designed at a time when cars are not connected, they are vulnerable to attacks. For example, the attacker can easy gains access to the internal network, based on CAN (Controller Area Network) protocol and thus manage to control airbag control system [9].

2.7. Identity Attack

Identity privacy ITS may refers to the privacy of a driver, passenger, pedestrian and so forth. The attacking party may try to extract information about personal data, location, actions, habits. An example of an identity attack is a case in which the attacking party manages to obtain information on how nicknames are assigned in VANET and thus track the location of a vehicle [9].

2.8. Eavesdropping

Eavesdropping is a classic passive attack in which the attacking party does not disrupt the communication process but manages to gain unauthorized access to information. Example: The malicious party may eavesdrop on the communication between the vehicle and the road

infrastructure during the payment of the toll and thus gain access to the user's bank account details [12].

2.9. Attack against Fog

Due to their physical characteristics (usually physically accessible) and limited resources in comparison to the Cloud, ITS's Fog components are difficult to protect and can be subject to various types of attacks. Example: Fog node summarizes and purifies data from sound and vibration sensors. By altering the aggregated information, the malicious party directly affects the data analysis algorithm for planning the organization of the road traffic [5,9].

2.10. AI Attacks

The attacks against AI could be related to data manipulation (Data poisoning attack), Environmental Perturbations or Policy manipulation. Example: In order to mislead the machine learning algorithm, the attacking party may select and send data so as to cause false trends in the model [9,13].

3. ITS Architecture and Security Challenges

The ITS can be seen as a sub-type of IoT and so it can be developed using similar approaches and architectures. The Figure 1 depicts the architecture contours of most IoT developments. It could also be applied in ITS [8].

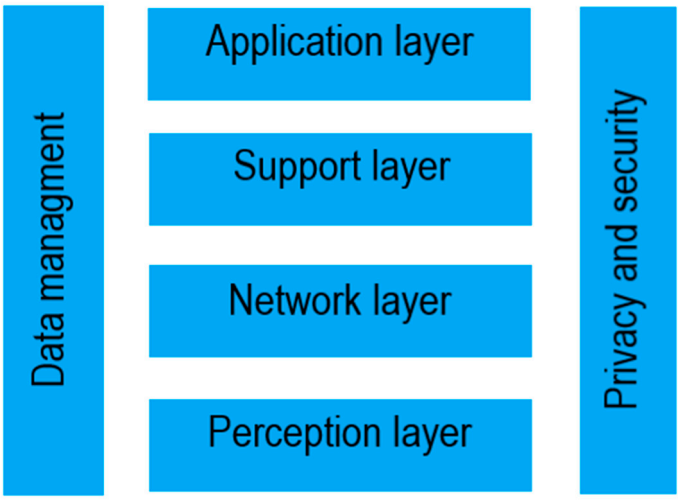

Figure 1. Internet of things (IoT) architecture outlines [8].

The presented architecture consists of four layers responsible for different functions of IoT. Applying this outlines in ITS gives each layer a more specific functions.

Perception layer of ITS encompasses users' smartphones, in-vehicles' sensors and infrastructure devices. Many of security issues at perception layer are concerned to configuration and initialization of the devices during manufacturing and internal vehicular network design, as in most cases it is not intended for connected cars [8,14].

Network layer is a complex alloy of wired and wireless technologies. One of the big cybersecurity questions at this layer is providing authentication of the nodes in VANET. Due to the need to protect personal data, authentication needs to be anonymous. The limited range of nodes and the strict time requirements introduce additional difficulties [2,3,6].

Among the developments for VANET architecture standards, two network technologies are outlined—the family of standards IEEE 1609 (Wireless Access in Vehicular Environment—WAVE),

based on 802.11 and the 3GPP standard (applicable for 4G and 5G LTE-Long Term Evaluation networks called Cellular Vehicle to Everything—C-V2X) [4,7,15].

WAVE describes authentication mechanism based on a list of hierarchical certificates. It specifies precise requirements for specific cryptographic primitives and does not provide an alternative. The issue here is that in dynamic situation and load network the procedure described in standard is not satisfying the time constraints. It require: the elliptic curve digital signature algorithm (ECDSA) and concrete elliptic curves P-256 and P256r1; the maximum size of the private key—32 bytes; AES-CCM (Advanced Standard Encryption in Counter Mode)—a symmetric encryption algorithm and the hash function SHA-256 [4,7,16].

C-V2X technology defines two modes of operation—mode 4 (Unmanaged Mode) and mode 3 (Managed Mode). The standard security mechanisms of LTE standards are applicable in Managed Mode. In Unmanaged Mode, security issues remain unresolved. The standard sets requirements for duplication protection, integrity, confidentiality and envisage the use of pseudonyms. It outlines the requirements but does not make recommendations for specific mechanisms [7,16].

The 5G philosophy is service oriented. Slicing Security as-a-Service or SSaaS, enables operators to provide differentiated and customized security package, including encryption algorithms, encryption parameters, capabilities for blacklist and whitelist configuration, authentication methods and isolation strength and so forth. [15].

At **support layer** the data is being processed in the Fog or Cloud depending on their temporal and spatial specifics and security considerations. As an emerging technology, Fog-based structures present new security challenges because the operation environments of distributed Fog systems are more difficult to protect than a centralized Cloud. The existing security and privacy measurements for cloud computing cannot be directly applied to the fog computing due to its features, such as mobility, heterogeneity and large-scale geo-distribution [5,8].

The **application layer** reflects the final interaction with the user, which can be expressed in information, warning and even activation of a certain system in the vehicle (in the case of unmanned vehicles). Before reaching the user the data acquired in the sensor layer can be processed in multiple locations. Depending on data semantics, security requirements and time constraints calculations can be done locally, in the vehicle itself, in road side units (RSU), at Fog or Cloud. The data in ITS meet all the characteristics of Big data, which is a precondition for applying Artificial Intelligence (AI). Its application into security-critical systems such as ITS must be carefully considered, as it is very vulnerable to a number of cyberattacks [1,8,15,17–19].

Table 1 summarizes the security issues addressed in this document, their respective architectural layers and the possible cyberattacks.

Table 1. Intelligent Transportation Systems (ITS) architecture, cybersecurity issues and attacks.

Architecture Layer	Security Issue	Cyberattack
Perception layer	Configuration and initialization of the devices during manufacturing; Internal vehicular network design;	Denial-of-Service; Spoofing; Internal vehicle network attack;
Network layer	Anonymous authentication in VANET;	Sybil Attacks; Denial-of-Service; Man-in-the-Middle; Eavesdropping; Routing attacks; Identity attack; Timing attack;
Support layer	Fog defense;	Attack against Fog;
Application layer	Complicated data model; AI defense.	Data poisoning; Environmental Perturbations; Policy manipulation.

4. Conventional Methods in ITS Cybersecurity

Although ITS are relatively new, many of the technologies they integrate have been tested in practice and the experience gained can be reused. In terms of security, some of the classic approaches will certainly play a key role. The effective approaches of defending support layer are: strong authentication, encrypted communication, key management, regular auditing and private network and secure routing [8,12,20,21].

Cryptographic methods are the heart of cybersecurity. The application of cryptographic techniques in the automotive industry has a history since 90s. Traditional algorithm and encryption standards are not completely suitable for ITS as they cannot meet the requirements of high throughput performance, low latency and reliability. Lightweight encryption has become a basic requirement in ITS [8,12].

Network segmentation is another classic approach that improves both network security and efficiency. When talking about ITS network segmentation, it should be taken into account that some of the nodes are mobile, dynamically joining and with anonymity requirements. In VANET, the separation of clusters from communicating cars would play an important role, thus building hierarchy in the network. Depending on the goals and the situation, different metrics can be taken into account—the behavioral characteristic, based on historical data, the resources, the location and so forth. [21].

In Reference [21] authors describe IoT security segmentation pattern. They take into account security level, attack surface, heterogeneity, identity, compliance, threats and overhead.

5. Innovative Approaches in ITS Cybersecurity

The introduction of technologies that were not originally designed to serve time-critical areas, as well as introduction of technologies from areas where cybersecurity is not directly related to users' physical security, leads to an increase in the vulnerability to cyberattacks in ITS. Borrowing technologies between different sub-areas in IoT is quite natural. In this section some innovative technologies that have found application in ITS or have found application in similar areas and their application in ITS is yet to be experimented with are presented. Given the multi-faceted nature of ITS, approaches to achieving cybersecurity objectives are multidimensional. Methods discussed in the Section 6 relate to the application layer and are holistic in nature, while this section discusses methods that have a local impact—in the network and perception layer. Blockchain, anonymous authentication in Fog and bloom filter are applicable in resource reduction in anonymous authentication of dynamic nodes in VANET. Security-by-contract and sensor fusion are applied in the sensor layer. Although data fusion can take place in any of the layers in the system, the sensor fusion approach is related to the perception layer, as the closer to the source the information is processed the less security risks exist [2,3,6,8,14,22–24].

5.1. Blockchain

Blockchain is an extremely dynamic technology in recent times. With regard to ITS, one of its main applications is in anonymous authentication solutions in VANET. The use of distributed storage can be very suitable for storing data of the legitimacy of nodes. The nodes decide whether to admit a new participant in the communication based on its reputation. In this way, malicious nodes are discouraged. Another option for applying a blockchain is upper architecture layers as a secure data warehouse. Although some of the described examples present MANET networks, the simulation results can be considered to be applicable to VANET as a subtype of MANET [6,22–25].

The authors of Reference [22] introduce the concept of "shortest, most reputed path" using the Ad hoc On-Demand Distance Vector (AODV) routing protocol for MANETs. They create a simulation, using Matlab, dividing the network into subnets in each of which there are mining nodes that monitor of the other nodes and add transactions to the blockchain. The blockchain contains information about the reputation of the nodes. The authors claim an approximately 12% improvement in overall packet delivery in the presence of routing attacks, compared to conventional routing algorithms in MANETs.

The authors of Reference [25] discuss the general importance of security in IoT systems, focusing on MANET. They describe a future development (similar to Reference [21])—blockchain-based OLSR (Optimized Link State Routing Protocol), taking into account not only the node's reputation but also its energy level.

In Reference [24] an overview of significant applications of blockchain technology and possible attacks is presented. To analyze the traffic behavior on the network, five virtual clients were created. The authors conclude that the problem of ensuring data security is not completely resolved. They emphasize the possibility of identifying traffic to blockchain technology using behavioral analysis and recommend hiding traffic and preventing the interception of traffic from this technology, including by behavioral analysis.

Reference [23] offers a different application of blockchain for IoT—SEBS (Secure Element Blockchain Stratagem). It applies blockchain in the data layer, combining it with hardware secure elements in the sensor layer. The conclusion is that the proposition can increase the performance of critical security operations by 31 times, all while reducing computational and memory overheads.

Reference [6] introduces blockchain with floating genesis block and its contribution to resolve the issue of continuously growing blockchain within the VANET/MANET networks. The authors offer a comparative analysis with other methods that reduce the time to decide on the connection of new nodes in VANET and conclude that this modification allows resolving the blockchain growth issue completely in case blocks are downloaded from trusted nodes. They note that the modification introduces an element of centralization of the system and make a proposal to mitigate this drawback.

5.2. Anonymous Authentication in Fog

As Fog nodes provide precious opportunities to protect the privacy of the consumers before personal sensitive data leave the edge. Fog technology is one of the solutions to the problem of anonymous authentication in VANET [2,8,14].

Reference [2] introduces fog computing for anonymous vehicle legitimation. The advantages of this solution are that do not need to authenticate all the RSUs in the driving period, thereby reducing the times of authentications between legitimate vehicles and RSUs. The system model of this study consists of three layers: the cloud layer, the fog layer and vehicles.

5.3. Bloom Filter

Bloom filter is another solution to the issue of reducing resources when using changing aliases.

Reference [3] presents validation of pseudonyms in VANET, based on Bloom Filter. Bloom Filter stores all certificates generated for a given period. Instead of requiring a response from a trusted party for each package received, a reference is made to the Bloom Filter, which refreshes over time. The disadvantage is that this method gives false positive results. The authors include auxiliary methods—requesting the trusted party and list of illegitimate participants.

5.4. Security by Contract

Security by contract paradigm is based on a description of the relevant features of the application and the relevant interactions with its host platform. This approach is a possible solution to many of the security tasks in the sensor layer, as it is also applicable to devices that are put into operation [14].

In Reference [14] is presented security solution for correctly defining rules in IoT devices applicable by a user, administrator or manufacturer. It consists of security contracts that can be verified against the security policy stored within the Fog node. By real smart home experiment, pseudo-code algorithms and a number of illustrative examples the authors motivate the necessity to develop such system.

5.5. Sensor Fusion

Sensor fusion can offset incorrect information from corrupting computations and reducing data ambiguity. A great advantage of this technology is that it allows the use of inexpensive sensors and

thus significantly reduces the final cost of the products without affecting the measurement result. Sensor fusion is already applied in practice in many modern automobiles [9].

6. An Intelligent Security in IoT

Due to the complexity of ITS an intelligent and proactive defense approach is a necessity. The methods described in this section relate to the holistic approach of ITS cybersecurity and have been successfully applied in security systems in other areas. In relation to ITS, they are mentioned on many sources as methods that will outline the overall appearance of ITS in the future but still the experimental results of their application in ITS are few. This is largely due to the fact that the development of the whole system is not mature enough. This section discusses examples of the application of artificial intelligence, machine learning, ontologies and game theory in security systems [8,15,17].

6.1. Artificial Intelligence

With the advent of IoT, AI is increasingly used in Intrusion Detection Systems (IDS), due to the increased risk to security and complexity of tasks. AI will definitely find a place in future ITS cybersecurity, due to the need for adaptive solutions to the rapidly changing system and the need for a holistic approach [11,17].

Reference [13] describes a novel hybrid Deep Learning and Dendritic Cell Algorithm (DeepDCA) in the context of an IDS. The authors argue that experimentation results show that DeepDCA demonstrate over 98.73% accuracy and low false-positive rate.

6.2. Machine Learning

Machine learning (ML) is the subset of AI that is most widely used in cybersecurity systems. Its weakness is that it is vulnerable in the training phase, so the training data set must be carefully selected. If a noise is inserted, the whole system can be compromised (Envision Attacks, Poisoning Attacks). It is necessary to create a strong classifier through proactive approaches. Due to this disadvantage, ML techniques are often used as an auxiliary mechanism [15,26].

Reference [27] presents automatic IP blacklisting applying linear regression techniques. The authors claims that it can reduce the incorrect blacklisting by nearly 90% and improve the time to eliminate malicious IP compared to human agents.

6.3. Ontology

Ontology is a promising tool to address heterogeneous issues, especially for unstructured data. The application of ontology to the IoT security domain is an emerging area [8,28].

In Reference [28] authors present a data-security ontology for IoT, from the perspective of data. It represents a common vocabulary describing the practical security aspects related to data access and exchange relevant to producers, consumers and intermediaries. Its objective is to provide relevant information about data provision, access and handling, as well as to regulations that may affect it and certifications and provenance.

6.4. Game Theory

Game theory is a powerful mathematical tool that has been successfully applied in the fields of cybersecurity and privacy [8,29].

In Reference [29] the proposed method combines reputation and game theory-based methods for selfish node detection in MANETs. It consists of several steps which are performed as games between nodes in a clustered network when sending or forwarding the node's data packets. Each player independently chooses their own strategy for forwarding or not forwarding. The experimental results have shown that the proposed method can detect selfish and malicious nodes efficiently, decrease the end-to-end delay of the data and consumption of node resources (energy, battery, memory, etc.).

The proposed approach gives the malicious and selfish nodes the second opportunity to cooperate with other nodes and thus improve the network performance.

7. Discussion

ITS is a complex multi-component system in which is sensible to cybersecurity and vulnerable in all its subsystems. In presented paper a four-layer model of IoT architecture that has been adapted to differentiate the issues more clearly is shown.

At perception layer Spoofing attacks result in incorrect data acquisition. Denial-of-Service can cause failure of any of the systems. The main issue at this layer is configuration and initialization of the devices during manufacturing and internal vehicular network design, which does not comply with the connection of vehicles in dynamic networks.

Security by contract concept is a promising technology at perception layer, especially with regard to issues related to changes and improvements in security strategies. Sensor fusion is successfully applied in practice in order to eliminate inaccurate information.

At network layer numerous of cyberattacks are possible due to dynamic topology of the VANETs. Sometimes the attacking party can act passively, for example eavesdropping. Black and gray hole attacks omit the re-transmission of packets and thus disrupt communication. Man-in-the-Middle attack spread modified data. Timing attack delay transmission of the data and this way it damages systems that rely on real-time response. Sybil rely on replacing the identity of a nodes, thus can cause Jamming or Denial-of-Service. Due to the possibility of Identity attack the authentication of the nodes is necessarily to be anonymous.

Different solutions with regard to anonymous authentication, are being sought to reduce the network and computing resources required for the continuous exchange of pseudonyms in VANET.

One of the fastest growing technologies that is being experimented in this area is blockchain. In addition to anonymous authentication, blockchain in ITS security could find application in upper architecture layers as a secure data warehouse. Another answer to the question of reducing resources in anonymous authentication is Fog computing. Keeping the vulnerable identity information of the nodes at the edge of the system would limit the risk of attacks. The use of several complementary technologies is a possible solution to the issue of resource-effective authentication. A good example of this is a bloom filter as a main method and a blacklist and a request to the legitimate party as an auxiliary methods.

At **support layer**, defense of fog-based structures is the main issue.

Conventional security methods as cryptography and network segmentation are the most appropriate solution for Fog defense. They need to be adapted to the needs of ITS.

At **application layer**, the main issues that security should focus on are description and standardization of the complex model of data and metadata and defense of systems, based on AI.

The possible attacks at this layer are Data poisoning, Environmental Perturbations and Policy manipulation.

Due to the complexity of ITS, an intelligent security strategy is required. AI, machine learning, ontologies and game theory are tools that have found application in cybersecurity solutions. Their application and adaptation to ITS needs to be studied in detail. Intelligent security often is based on cooperation between cybersecurity specialists and a variety of intelligent security solutions.

An example of collaboration between experts and automated cybersecurity approaches is a system for cyber-risk scenario analysis for connected and automated vehicles (CAV) based on Bayesian Network (BN) presented in Reference [30]. In the initial phase of establishment, BN is constructed based on expert judgment. Quantitative and qualitative information from NVD (National Vulnerability) for 88,438 known vulnerabilities were used to refine BN, using machine learning methods. The performed tests demonstrate nearly 100% prediction accuracy of the quantitative risk score and qualitative risk level. Proposed methodology is applied to CAV GPS systems.

Another example of simulation analysis that can help in developing methodologies to resist or mitigate the effects of the attacks in a CAV platoon, such as intrusion detection, privacy protection and counteracting control methods anomaly detection is presented in Reference [31]. To understand cyberattack effect propagation the authors use a directed graph model, presented with adjacency matrix. For the simulation it is assumed that platoon of 15 CAVs is traveling on a straight road segment without overtaking and lane changing and incorporate the effects of three types of attacks (bogus messages, replay/delay and collusion attack). It was concluded that cyberattacks could influence vehicles unnecessary delay, extremely small gap, abrupt acceleration/deceleration and rear-end collisions. The authors propose the cooperative intelligent driver model.

The two described studies are good examples of initial development of ITS cybersecurity methodologies that need to be considered and integrated into a comprehensive system and tested into real vehicles.

Table 2 summarizes the approaches considered for ITS cybersecurity in accordance with the problems they solve, cyberattacks and the architectural layer to which they correspond.

Table 2. ITS architecture and cybersecurity issues and approaches.

Architecture Layer	Security Issue	Cyberattack	Security Approach
Perception layer	Configuration and initialization of the devices during manufacturer; Internal vehicular network design;	Denial-of-Service; Spoofing;	Security by contract; Sensor fusion;
Network layer	Anonymous authentication in VANET;	Sybil Attacks; Denial-of-Service; Man-in-the-Middle; Eavesdropping; Routing attacks;	Blockchain; Reputation based models; Bloom filter combined with auxiliary methods; Game theory;
Support layer	Fog defense;	Attack against Fog;	Authentication; Encryption; Key management; Regular auditing;
Application layer	Complicated data model; AI defense.	Data poisoning; Environmental Perturbations; Policy manipulation.	Blockchain; AI; Machine learning; Ontology; Game theory.

8. Conclusions and Future Work

ITS are complex, time-critical systems in which the physical safety of road users and the efficiency of transport services directly depend on the provision of cybersecurity. Although developments for ITS standards exist, the imposition of a comprehensive standard as well as the creation of a security strategy is not yet a fact. The interoperability between the various standards within the ITS and the interaction with the surrounding world (Smart Cities, IoT) needs to be well considered and tested.

Some of the described technologies such as blockchain, lightweight cryptographic methods, network segmentation and sensor fusion will certainly find a place in the appearance of ITS, although more experimental results are needed, as well as tests on how they will fit into the overall system.

Another part of the discussed technologies is in the initial stage of research regarding their application in ITS. AI and Machine Learning are mentioned in many sources as an important technology that will determine the vision of ITS. The advantages of utilizing such approaches are greatly publicized, while the security implications of their integration with ITS remain not studied

enough. On the other hand, experimental results from the application of these technologies in ITS security systems are needed. Another technologies that is expected to be developed under ITS domain are Game theory and Security-by-Contract. They are successfully applied in IoT cybersecurity solutions and is likely to find a place in ITS cybersecurity.

Author Contributions: Conceptualization, N.K. and T.M.; investigation, T.M.; resources, T.M.; writing—original draft preparation, T.M.; writing—review and editing, N.K.; visualization, T.M.; supervision, N.K.; funding acquisition, N.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the European Regional Development Fund within the OP "Science and Education for Smart Growth 2014–2020", Project CoC "Smart Mechatronic, Eco- And Energy Saving Systems And Technologies", No BG05M2OP001-1.002-0023 233.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript or in the decision to publish the results.

References

1. Coppola, P.; Silvestri, F. Autonomous vehicles and future mobility solutions. In *Autonomous Vehicles and Future Mobility*; AET Series; Elsevier: Amsterdam, The Netherlands, 2019.
2. Han, M.; Liu, S.; Ma, S.; Wan, A. Anonymous-authentication scheme based on fog computing for VANET. *PLoS ONE* **2020**, *15*, e0228319. [CrossRef] [PubMed]
3. Jin, H.; Papadimitratos, P. Proactive certificate validation for VANETs. In Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016.
4. IEEE. *1609.2-2016 IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*; Revision of IEEE Std 1609.2-2013; IEEE: Pictasaway, NJ, USA, 2016; pp. 1–240.
5. Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. *J. Cloud Comput. Adv. Syst. Appl.* **2017**, *6*, 19. [CrossRef]
6. Busygin, A.G.; Kalinin, M.; Konoplev, A. Supporting connectivity of VANET/MANET network nodes and elastic software-configurable security services using blockchain with floating genesis block. In *Proceedings of the IV International Scientific Conference 'the Convergence of Digital and Physical Worlds: Technological, Economic and Social Challenges' (CC-TESC2018), St. Petersburg, Russia, 16–18 May 2018*; SHS Web of Conferences Volume 44; EDP Sciences: Les Ulis, France, 2018.
7. Mir, Z.H.; Filali, F. LTE and IEEE 802.11p for vehicular networking: A performance evaluation. *J. Wirel. Commun. Netw.* **2014**, *2014*, 89. [CrossRef]
8. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
9. Hahn, D.A.; Munir, A.; Behzadan, V. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. *IEEE Intell. Transp. Syst. Mag.* **2019**, *1*. [CrossRef]
10. Katrakazas, C.; Theofilatos, A.; Papastefanatos, G.; Härri, J.; Antoniou, C. *Cyber Security and Its Impact on Cav Safety: Overview, Policy Needs and Challenges*; Elsevier: Amsterdam, The Netherlands, 2020.
11. Sanguino, T.D.J.M.; Domínguez, J.M.L.; Baptista, P.D.C. *Cybersecurity Certification and Auditing of Automotive Industry*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 95–124.
12. Jadoon, A.K.; Wang, L.; Li, T.; Zia, M.A. Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wirel. Commun. Mob. Comput.* **2018**, 1–15. [CrossRef]
13. Vähäkainu, P.; Lehto, M. Artificial intelligence in the cyber security environment. In Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS 2019, Stellenbosch, South Africa, 28 February–1 March 2019; Available online: https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment (accessed on 12 October 2020).
14. Giaretta, A.; Dragoni, N.; Massacci, F. IoT Security Configurability with Security-by-Contract. *Sensors* **2019**, *19*, 4121. [CrossRef] [PubMed]
15. Huawei Technologies Co., Ltd. *5G Security Architecture White Paper*; Huawei Technologies Co., Ltd.: Shenzhen, China, 2017.

16. Mandy, C.; Mahgoub, I. Implementation of the WAVE 1609.2 Security Services Standard and Encountered Issues and Challenges. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 13–18. [CrossRef]
17. Aldhaheri, S.; AlGhazzawi, D.M.; Cheng, L.; Alzahrani, B.A.; Al-Barakati, A. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System. *Appl. Sci.* **2020**, *10*, 1909. [CrossRef]
18. Gordeychik, S.; Nikolaev, A.; Kolegov, D. Measuring Artificial Intelligence and Machine Learning Implementation Security on the Internet, Project: AI Security. 2019. Available online: https://www.researchgate.net/publication/337771481_Measuring_Artificial_Intelligence_and_Machine_Learning_Implementation_Security_on_the_Internet (accessed on 12 October 2020).
19. Liang, F.; Hatcher, W.G.; Liao, W.; Gao, W.; Yu, W. Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access* **2019**, *7*, 158126–158147. [CrossRef]
20. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
21. Fernández, E.B.; Washizaki, H.; Yoshioka, N. Abstract and IoT security patterns. In Proceedings of the 8th Asian Conference on Pattern Languages of Programs (PLoP'19), Tokio, Japan, 20–22 March 2019.
22. Careem, M.A.A.; Dutta, A. Reputation based Routing in MANET using Blockchain. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 7–11 January 2020; pp. 1–6.
23. Deshpande, V.; Das, T.; Badis, H.; George, L. SEBS: A Secure Element and Blockchain Stratagem for Securing IoT. In Proceedings of the 2019 Global Information Infrastructure and Networking Symposium (GIIS), Paris, France, 18–20 December 2019; pp. 1–7. [CrossRef]
24. Elagin, V.; Spirkina, A.; Levakov, A.; Belozertsev, I. Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security. *Futur. Internet* **2020**, *12*, 68. [CrossRef]
25. Mouchfiq, N.; Habbani, A.; Benjbara, C. Blockchain Security in MANETs. Open Science Index 154. *Int. J. Comput. Inform. Eng.* **2019**, *13*, 546–550. [CrossRef]
26. Rahimi, N.; Maynor, J.; Gupta, B. Adversarial Machine Learning: Difficulties in Applying Machine Learning to Existing Cybersecurity Systems. *EPiC Series Comput.* **2020**, *69*, 40–47. [CrossRef]
27. Jeon, D.; Tak, B. BlackEye: Automatic IP blacklisting using machine learning from security logs. *Wirel. Netw.* **2019**, 1–12. [CrossRef]
28. Gonzalez-Gil, P.; Martinez, J.A.; Skarmeta, A. Lightweight Data-Security Ontology for IoT. *Sensors* **2020**, *20*, 801. [CrossRef] [PubMed]
29. Nobahary, S.; Garakani, H.G.; Khademzadeh, A.; Rahmani, A.M. Selfish node detection based on hierarchical game theory in IoT. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*. [CrossRef]
30. Sheehan, B.; Murphy, F.; Mullins, M.; Ryan, C. Connected and autonomous vehicles: A cyber-risk classification framework. *Transp. Res. Part A* **2019**, *124*, 523–536. [CrossRef]
31. Wang, P.; Wu, X.; He, X. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. *Transp. Res. Part C* **2020**, *115*, 102625. [CrossRef]