doi:10.20944/preprints202008.0082.v1

*Review*

# Cybersecurity in Intelligent Transportation Systems

**Teodora Mecheva [1] and Nikolay Kakanakov [2,*]**

[1] Technical University of Sofia, Plovidv branch; teodora.mecheva@tu-plovdiv.bg
[2] Technical University of Sofia, Plovidv branch; kakanak@tu-plovdiv.bg
* Correspondence: kakanak@tu-plovdiv.bg; Tel.: +359-895-587-568 (N.K.)

**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 been trying to find their place in ITS security strategies recently. The list of innovative approaches includes blockchain, bloom filter, fog computing, artificial intelligence, game theory, and ontologies. In conclusion, a correspondence 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

Intelligent Transportation Systems (ITS) are complex multilateral systems aimed at solving problems of transport safety and road traffic efficiency. They are characterized by strict time requirements, dynamics and large volumes of data. Ensuring security in ITS is a complex task on which the safety and efficiency of transportation depends [1].

Although there is no established standard for a complete ITS architecture, most IoT developments require several layers that describe the general contours of such systems (Figure 1). Cybersecurity in a system as complex as ITS takes place on all levels. On the other hand, it should be considered that ITS will be part of a larger ecosystem – that of the smart city and even the IoT [2].

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, e.g. direction, acceleration, speed, road conditions, weather conditions, etc. [3-6].

## 2. ITS architecture and security challenges

The ITS can be seen as a subtype of IoT and so the can be developed using similar approaches and architectures. The Figure 1 depicts the contours of most IoT developments. It could also be applied in ITS [2].

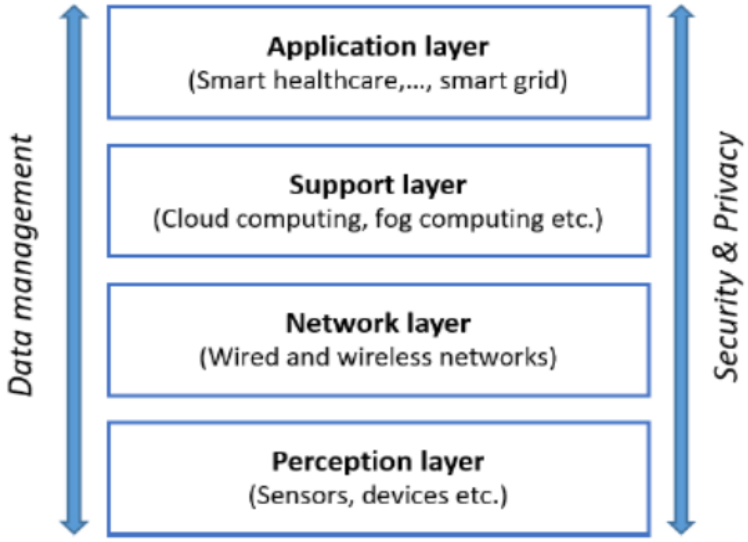

**Figure 1.** IoT outlines [2]

The outlines 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 [2, 7].

**Network layer** is a complex alloy of wired and wireless technologies. One of the big cybersecurity questions at this layer is providing anonymous authentication in a VANET. The limited range of nodes and the strict time requirements introduce additional difficulties [3, 4, 8].

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) [5, 9, 10].

WAVE describes authentication mechanism based on list of hierarchical certificates. It specifies precise requirements for specific cryptographic primitives and does not provide an alternative. The issue here is in dynamic situation and load network the procedure described in standard is not satisfying the time constraints [5, 10, 11].

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 [9, 10].

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 etc [9].

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 [2, 6].

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, 2, 9, 12, 13, 14].

The most common security issues on each layer of the presented outlines are shown on Table 1.

**Table 1.** Comparison of security issues and the architectural layers in ITS

| Architecture layer | Title 2 |
|---|---|
| Perception layer | Configuration and initialization of the devices during manufacturing |
| Network layer | Anonymous authentication in VANET |
| Support layer | Fog defense |
| Application layer | Complicated data model, AI defense |

## 3. 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 defensing support layer are strong authentication, encrypted communication, key management, regular auditing, and private network and secure routing [2, 15, 16, 17].

*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 [2, 16].

*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 [17].

In [17] authors describe IoT security segmentation pattern. They take into account security level, attack surface, heterogeneity, identity, compliance, threats, and overhead.

## 4. Innovative approaches in ITS cybersecurity

As ITS are multi-faceted, cybersecurity in such systems must also be multidimensional. In addition to the application of conventional methods, some innovative approaches are needed.

### *4.1. Blockchain*

Blockchain is an extremely dynamic technology in recent times. With regard to ITS, one of its main applications is in anonymous authentication solutions. The use of distributed storage can be very suitable for storing data on 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 in the data layer [8, 18, 19, 20, 21].

The authors of [21] 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 the actions 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 [18] discuss the general importance of security in IoT systems, focusing on MANET. They describe a future development (similar to [21]) - blockchain-based OLSR (Optimized Link State Routing Protocol), taking into account not only the node's reputation but also its energy level.

In [20] is presented overview of significant applications of blockchain technology and possible attacks. 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.

[19] 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.

[8] 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.

### *4.2. 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, 3, 7].

[3] 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.

### *4.3. Bloom filter*

Bloom filter is another solution to the issue of reducing resources when using changing aliases. [4] presents validation of pseudonyms 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.

### *4.4. 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 [7].

In [7] 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. An intelligent security in IoT

Due to the complexity of ITS an intelligent and proactive defense approach is a necessity. Intelligent security is based on co-operation between cybersecurity specialists and a variety of intelligent security solutions [9, 22].

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

**Machine learning** (ML) is the sub set 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 [9, 23].

[24] 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.

**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 [2, 25].

In [25] 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.

**Game theory** is a powerful mathematical tool that has been successfully applied in the fields of cybersecurity and privacy [2, 26].

In [26] the proposed method combines reputation and game theory-based methods for selfish node detection in MANETs. It consists of several steps that is performed 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.

## 6. Conclusions

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.

The open issues in ITS security are the lack of suitable methods for: configuration and initialization of the devices during manufacturing; anonymous authentication of nodes in VANET; defense of fog-based structures; description and standardization of the complex model of data and metadata and defense of systems, based on AI. Conventional security methods as cryptography and network segmentation need to be adapted to the needs of ITS. Innovative approaches are being experimented within security bottlenecks. 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. 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. Security by contract concept is a promising technology at perception layer, especially with regard to issues related to changes and improvements in security strategies.

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

**Table 2.** ITS cybersecurity architecture, issues and approaches.

| Architecture level | Security issue | Security approach |
|---|---|---|
| Perception layer | Configuration and initialization of the devices during manufacturing | Security by contract |
| Network layer | Anonymous authentication in VANET | Blockchain; reputation based models; Fog computing; bloom filter combined with auxiliary methods; Game theory |
| Support layer | Fog defense | Authentication, encryption, key management, regular auditing, private network and secure routing |
| Application layer | Complicated data model, AI defense | Blockchain; AI; Machine learning; Ontology; Game theory |

**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", № BG05M2OP001-1.002-0023

**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. P. Coppola and F. Silvestri, Autonomous vehicles and future mobility solutions. Included in the Book "Autonomous vehicles and Future mobility", doi:10.1016/B978-0-12-817696-2.00001-9: AET series – Elsevier, 2019.
2. L. CUI, Security and Privacy in Smart Cities: Challenges and Opportunities, Vols. 6, pp. 46134-46145, doi: 10.1109/ACCESS.2018.2853985: IEEE Access, 2018.
3. M. Han, S. Liu, S. Ma and A. Wan, Anonymous-authentication scheme based on fog computing for VANET, vol. 15(2), doi: e0228319, 2018.
4. H. Jin and P. Papadimitratos, Proactive certificate validation for VANETs, doi: 10.1109/VNC.2016.7835974: IEEE Vehicular Networking Conference (VNC), 2016.
5. IEEE, IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, Vols. 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp.1-240, doi: 10.1109/IEEESTD.2016.7426684: IEEE Std, 2016.
6. S. Khan, S. Parkinson and Y. Qin, Fog computing security: a review of current applications and security solutions, doi: 10.1186/s13677-017-0090-3: Journal of Cloud Computing: Advances, Systems and Applications, 2017.

7. A. Giaretta, N. Dragoni and F. Massacci, IoT Security Configurability with Security-by-Contract, doi: 19. 4121. 10.3390/s19194121: Sensors, 2019.
8. A. Busygin, M. Kalinin and A. Konoplev, Supporting connectivity of VANET/MANET network nodes and elastic software-configurable security services using blockchain with floating genesis block, doi: 10.1051/shsconf/20184400020: SHS Web of Conferences, 2018.
9. HUAWEI TECHNOLOGIES CO., LTD., 5G Security Architecture White Paper, online: https://www.huawei.com/en/industry-insights/technology/5g-security-architecture-white-paper, 2017.
10. Z. H. Mir and F. Filali, LTE and IEEE 802.11p for vehicular networking: a performance evaluation, 1687-1499-2014-89: J Wireless Com Network, 2014.
11. C. Mandy and I. Mahgoub, Implementation of the WAVE 1609.2 Security Services Standard and Encountered Issues and Challenges, Vols. 9. pp. 13-18, doi: 10.1109/UEMCON.2018.8796755: Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018.
12. S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani and A. Al-Barakati, DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System, Vols. 10(6), 1909, doi: 10.3390/app10061909: Applied Sciences, 2020.
13. S. Gordeychik, A. Nikolaev and D. Kolegov, Measuring Artificial Intelligence and Machine Learning Implementation Implementation Security on the Internet, doi: 17. 10.13140/RG.2.2.15662.66888: Project: AI Security, 2019.
14. F. iang, W. G. Hatcher, W. iao, W. Gao and W. Yuy, Machine Learning for Security and the Internet of Things: the Good, the Bad, and the Ugly, doi: 10.1109/ACCESS.2019.2948912: IEEE Access, 2019.
15. M. MUKHERJEE, R. MATAM, L. SHU, L. MAGLARAS, M. A. FERRAG, N. CHOUDHURY and V. KUMAR, Security and Privacy in Fog Computing: Challenges, doi: 10.1109/ACCESS.2017.2749422: IEEE Access, 2017.
16. A. . K. Jadoon, L. Wang, T. Li and M. A. Zia, Lightweight Cryptographic Techniques for Automotive Cybersecurity, Vols. 1-15, doi: 10.1155/2018/1640167: Wireless Communications and Mobile Computing, 2018.
17. E. B. Fernández, H. Washizaki and N. Yoshioka, Abstract and IoT security patterns, online: https://pl.csie.ntut.edu.tw/asianplop2019/papers/2.1.pdf: 9th Asian Conference on Pattern Languages of Programs (PLoP'19), 2019.
18. M. A. A. Careem and A. Dutta, Reputation based Routing in MANET using Blockchain, pp. 1-6, doi: 10.1109/COMSNETS48256.2020.9027450: International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020.
19. V. Deshpande, T. Das, H. Badis and L. George, SEBS: A Secure Element and Blockchain Stratagem, pp. 1-7, doi: 10.1109/GIIS48668.2019.9044957: Global Information Infrastructure and Networking Symposium, 2019.
20. V. Elagin, A. Spirkina, A. Levakov and I. Belozertsev, Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security, vol. 12. 68, doi:10.3390/fi12040068: Future Internet, 2020.
21. N. Mouchfiq, A. Habbani, and C. Benjbara, Blockchain Security in MANETs, Vols. 13(10), 546 – 550, Open Science Index 154, doi:10.5281/zenodo.3566283: International Journal of Computer and Information Engineering, 2019.
22. P. Vähäkainu and M. Lehto, Artificial intelligence in the cyber security environment, https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment: International Conference on Cyber Warfare and Security ICCWS2019, 2019.
23. N. Rahimi, J. Maynor and B. Gupta, Adversarial Machine Learning: Difficulties in Applying Machine Learning to Existing Cybersecurity Systems, Vols. 69, p.40-47, doi: 14. 10.29007/3xbb: EPiCSeriesinComputing, 2020.
24. D. Jeon and . B. Tak, BlackEye: automatic IP blacklisting using machine learning from security logs, doi: 15. 10.1007/s11276-019-02201-5: Wireless Networks, 2019.
25. P. Gonzalez-Gil, J. A. Martinez and A. F. Skarmeta, Lightweight Data-Security Ontology for IoT, doi: 10.3390/s20030801: Sensors 2020, 2020.
26. S. Nobahary, H. G. Garakani2, A. Khademzadeh and A. M. Rahmani1, Selfish node detection based on hierarchical game theory in IoT, doi: 10.1186/s13638-019-1564-4 : EURASIP Journal on Wireless Communications and Networking, 2019.