information

MDPI

Review

Forecasting Issues of Wireless Communication Networks' Cyber Resilience for An Intelligent Transportation System: An Overview of Cyber Attacks

Mikhail Buinevich [1,2] **and Andrei Vladyko** [1,*]

[1] R&D Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Prospekt Bolshevikov 22-1, Saint Petersburg 193232, Russia; bmv1958@yandex.ru

[2] Department of Applied Mathematics and IT, Saint-Petersburg University of State Fire Service of Emercom of Russia, Moskovskiy prospekt 149, Saint Petersburg 196105, Russia

* Correspondence: vladyko@sut.ru

Received: 18 November 2018; Accepted: 10 January 2019; Published: 14 January 2019

Abstract: During the last decade there has been an essential development of wireless communication technologies for intelligent transportation system (ITS) applications for motor transport; these advanced infocommunication technologies are called vehicular ad hoc networks (VANET). VANET/ITS, in particular, inform and warn drivers about possible obstacles, and also the possibility of how to organize coordinated actions. Therefore, any violation of its functioning by cyber attacks automatically influences the safety of people and automotive engineering on the road. The purpose of this article is to provide an analytical overview of cyber attacks on VANET/ITS, presented in state-of-the-art publications on this topic by the prediction of its cyber resistance. We start with an analysis of the top 10 cyber threats, considered according to the following schemes: attack mechanism, vulnerability, damage, object of attack, and a counter measure. We then set out a synergistic approach for assessing the cyber resistance of the forward-looking VANET/ITS conceptual model, formed by the merger of the internet of vehicles and software-defined networking technology. Finally, we identify open issues and associated research opportunities, the main ones being the formalization of threats, vulnerability stratification, the choice of the level of network management centralization and, last but not least, the modeling and prediction of VANET/ITS cyber resistance.

Keywords: intelligent transportation systems; VANET; cyber resilience; synergetic approach; forecasting

1. Introduction

Developed countries around the world (for example, the USA, European Union member states, Japan, China, and Russia) are actively moving ahead in the direction of the digitalization of the economy, and in particular the transport systems that inevitability lead to the integration of means of communication which are built in vehicles (on-board unit, OBU) and infrastructure objects (roadside unit, RSU). During the last decade there has been an essential development of wireless communication technologies for intelligent transportation system (ITS) applications for motor transport; these advanced infocommunication technologies are called the vehicular ad hoc network (VANET). It is expected that the communication of vehicles with each other (vehicular to vehicular, V2V), with infrastructure (vehicular to infrastructure, V2I), and vulnerable participants of traffic will bring essential benefit from the point of view of safety and comfort; these methods can also promote improvement and more competent traffic management, provide the best way to prevent or reduce traffic jams, and also save fuel and thus reduce emissions [1,2]. These modes of communication are summarized by the term vehicle to everything (V2X).

VANET/ITS, in particular, informs and warns drivers about possible obstacles (repair work, speed limits, etc.) and also provides possibilities about how to organize coordinated actions (change of lanes, priority way on junctions, etc.). Therefore, any violation of its functioning automatically influences the safety of people and automotive engineering on the road: accordingly, this makes issues of the cyber resilience of VANET/ITS urgent. Authors consider cyber resilience as VANET's capability to provide and maintain an acceptable level of service of requirements of ITS for V2X-exchange of problem-oriented information in the conditions of destructive influences (for example, cyber attacks). In [3], the authors put forward a similar thesis. The increasing number of publications concerning various aspects of the cyber resilience of VANET/ITS, and the fast growth of revealed cyber threats (including zero-day threats) immature (i.e., in the conditions of deficiency of "best practice"), almost innovative cyber system creates a certain paradoxical situation that demands scientific judgment. The first step in this direction is the identification of problematic issues and forecasting of the cyber resilience of ITS telecommunication components.

2. Variants of Creating Cyber-Resilient Vehicular Ad Hoc Networks/Intelligent Transportation Systems (VANET/ITS)

In recent years, an extensive set of variants for the creation and development of VANET have been investigated. Analysis from [4] allows the identification of the main candidates to be telecommunication components of ITS in the context of supplying cyber security. Historically, the first is Wi-Fi technology according to the IEEE 802.11p standard, for which a special band in the region of 5.9 GHz is allocated and cheap chips are mass-produced. The large-scale "field" tests which were carried out in the USA and various European countries showed that VANET/ITS on this technology has a low delay (in the range of milliseconds), can cope with high relative speed between transceivers (up to 200 km/h and above), has high dynamics of information collection from nearby objects (dynamic topology of network), maintains considerable network loading (by means of constant periodic transmission of messages to several participants and a large number of transceivers in scenarios of the overloaded traffic), and is capable of working at a considerable distance (from several hundred meters to 1 km) and in conditions where direct visibility is lacking (by means of routing with several transitions by the use of other mobile knots and knots of transport infrastructure). In response to high standards of safety, the USA's department of transport has firmly adopted a position of introduction of the standard 802.11p, having initiated the process of rule-making for the mandate on expansion of communications of V2V on the basis of dedicated short-range communications (DSRC). They consider that the mandate will support producers in effective advance forward and will help to develop the critical mass of the equipped vehicles [5].

As the strong competitor of DSRC/802.11p, the 4G cellular communication technology (formally called long-term evolution for vehicular, LTE-V) is being considered by the European community; the Automotive Association 5GAA intends to promote it for corporate ITS (C-ITS). However, according to the results of comparative research conducted by specialists from the Dutch company NXP Semiconductors together with Israeli partners from Autotalks [6], nowadays the situation of using LTE-V as a telecommunication component of C-ITS seems to be less common. When comparing IEEE 802.11p with LTE-V2X, they highlight several important facts of both technological and economic sense. Firstly, the offered LTE-V2X technology is the derivative of a technology cellular ascending communication line which maintains similarity to the current LTE systems: the structure of a shot, an interval between bearing, requires the accuracy of hours and the concept of the block of resources, and some of them—these properties are not adapted for options of use of vehicles, but are rather inherited from the existing cellular technologies. Secondly, commercially available LTE-V2X cannot use the presence of the standard LTE modem in the car, as various safety and technological requirements strongly require that the LTE-V2X domain, crucial for safety, has to be separated from the "entertaining" domain of the standard LTE modem.

The modern technical policy of C-ITS focuses on the strengths of each technology and forcing them to work together with the purpose of providing the best decision for VANET/ITS. Therefore, the European Commission has expressed the need for a "full hybrid communication mix" on board vehicles for ensuring cyber security with the certain coordinated model of trust (trust models for C-ITS). One variant, for example, is in considerable degree to reserve capacity 802.11p for V2V communication connected with safety and to include some important messages of I2V, such as repeated transfer (replay) of the corresponding messages in conditions where direct visibility is lacking and to leave contact of I2V, less critical on time, with the cellular domain. A considerable part of this functionality will already be possible with the use of modern 4G technology; however it is quite obvious that the current 4G/LTE cellular technology cannot answer the strict requirements for communication of V2X connected with cyber security. At the same time, the supporters of cellular communication for ITS point to fifth generation mobile communication (5G) as being superior in productivity and safer than IEEE 802.11p [7].

3. Top 10 VANET/ITS Cyber Threats

Based on our analysis of the numerous sources describing critical topics of information security in VANET/ITS networks, we compiled the following list of the most serious cyber threats facing such networks:

- Broadcast tampering [8];
- DoS (Denial of Service) [9–17];
- Tracking [10,12,18–29];
- Routing [10,15,30–32];
- Tampering hardware [8,15];
- Sybil attack [18,26,27,31,33–39];
- Traffic analysis [10,15,19,25,40–44];
- Jamming [16,45];
- GPS spoofing/position faking [11,20,31,46–53];
- Timing attack [12,14,31];
- Message tampering/suppression/fabrication [9,20,21,38,39,42,46,54–61];
- Man in the middle [14,31,46,55,62–64];
- Brute force [26,32,65];
- Node impersonation [10,15,20,24,26,34,36,55,66,67];
- Replay [10,20,38,68];
- Illusion attack [11,20,46];
- Key and/or certificate replication [12,18,26,35,37,54,69–72];
- Malware spamming [15,36,73];
- Loss of event traceability [31,36,54], etc.

Such an abundance of threats implies their systematization and structuring. The authors of the report "VANET/ITS Cybersecurity Threats: Analysis, Categorization and Forecasting" at the 2018 EIConRus [74] critically analyzed the approaches to classification presented in the relevant reviews [8,75–77], and suggested all VANET/ITS threats, along with "classical" signs of a violation of a property's information resources, such as confidentiality, integrity and accessibility, or their combinations should be also identified by the main elements of ITS—vehicles, transport infrastructure, and their information technology interface interaction (in the sense of a wireless network)—as objects of attack.

In order to obtain a representative image of the topical area, we compiled the conditional "top 10" threats (ordered by the number of references that can be conventionally considered the primary taxonomy of cyber attacks on this topic) from the above list. We carried out the analysis according to the canonical scheme for information security: the attack mechanism–the exploited vulnerability–information security damage–object of attack–countermeasure.

3.1. Message Tampering/Suppression/Fabrication—Attacks to the Network Messages

A message tampering attack is directed to the violation of integrity of the networked messages: the malefactor modifies messages of OBU–OBU and OBU–RSU, while at the same time falsifications can be both a request of the application and a reply to the request. A message suppression attack is directed at the violation of confidentiality of the networked messages: the malefactor carries out a selection of packages and broadcasts them in the network; strange users, who do not take part in valid packages exchange, and have access to this network; packages, in particular, may contain information relating to the safety of a knot. A message fabrication attack is directed to the violation of integrity and confidentiality of the network messages: the malefactor broadcasts untrue reports in network; in this way the malefactor can acquire the right of priority journey, non-authorized access to system resources and confidential data (passwords, logins of other knots). Thus, the attack is aimed at the wireless network. Similar to 'traffic analysis' that is described below, it is generally used for carrying out the following cascade of attacks to all elements of the intellectual transport system. The countermeasure were not found in the reviewed sources; it is possible to assume encryption of the networked packages and the use of digital certificates for the authentication of a knot.

3.2. Tracking—Unauthorized Access to Identification Information on a Knot

This attack is directed at tracking the location of the vehicle during some period of time in order to obtain detailed information on a knot. It is aimed at the violation of data confidentiality of a legitimate knot since the malefactor seeks to intercept them and to use in the purposes. The task can be reduced to the calculation of coordinates by the analytical way. The received coordinates can be used by malefactors for subsequent physical attacks, such as hijacking of the vehicle (for example, a secure cash delivery vehicle). The countermeasure are not found in the reviewed sources.

3.3. Sybil Attack—Destruction of Network Reputation by Cloning of False Identifiers

By exploiting a vulnerability of a simple multiple fake of the identifier, the malefactor creates clones of identification data for exerting a disproportionately large influence on a network, repeatedly imitating the functioning of valid knots. The attack causes direct damage to network availability, littering traffic with untrue reports, and also increases the probability of sending data through the malefactor's knot (see "man in the middle" attack, below) that potentially leads to confidentiality violation, because the malefactor will read the traffic which is not intended for them. By means of this attack the malefactor can also influence integrity, for example to send false reports about the road situation. The attack is directed at transport infrastructure (regarding the algorithms which make certain decisions on the basis of reputation estimates from system participants). Therefore, for example, the fake-identifiers-of-vehicles set is localized moving in some area, and will make a traffic jam visible for assessment subsystems of a road situation. This may cause other subsystems to relieve road traffic (for example, by an increase in the duration of a green traffic light signal) and to construct alternate routes for the traffic. Nevertheless, equipment will be physically absent on the road, and malefactors can, therefore, use it for a free journey. Countermeasure include the creation of the confidential channel (for example, due to the validation of identification data).

3.4. DoS (Denial of Service)

This is the most known attack for the majority of networks. Its purpose is to finish VANET/ITS fully or to increase delays in the network that will make it impossible or complicated for legitimate users to obtain information. As the information in vehicle wireless networks becomes outdated very quickly, even small delays can set to zero the work of one segment, since at the time of obtaining information, a road situation will already be different. This attack directly reduces network availability and has many variations. Many researchers refer to DoS all the attacks as routing and/or consuming the resources.

The attack is aimed at wireless networks due to the creation of a huge amount of information (not necessarily false) demanding from VANET/ITS of the maximum quantity of resources for its processing; for example, multiple sending signals of the road accidents and repair work that arise will force the intellectual transport system to constantly re-estimate the road situation and recalculate optimum routes. At the moment there are many methods for counteracting DoS attacks, however their efficiency is still doubtful.

3.5. Node Impersonation—Substitution of Identification of the Participant of Traffic

This attack is implemented by substitution by the malefactor of the MAC- and IP addresses to addresses of a valid knot. In order to receive identification of other knots, the malefactor uses the corresponding spoofing. If there is no authentication, the attacker can send the fake report on behalf of another knot, thereby breaking integrity. For example, the malefactor speaks on behalf of the ambulance to get the priority drive. At the return operation, i.e., obtaining the message intended for the car with the required MAC and IP addresses, confidentiality will be broken. The main subject of the attack is the vehicle, because substitution by the malefactor of transport infrastructure knots (for example, traffic lights) will allow confidential information to be obtained about the vehicle.

At the same time, the substitution of the address of special purpose vehicles (for example, ambulances or fire trucks) will allow the transfer of the modified information to transport infrastructure, having ensured special traffic conditions ("the green road", etc.). Countermeasures include authentication based on certificates, and dynamic addresses.

3.6. Key and/or Certificate Replication—Unauthorized Identification in System

This attack involves the use of duplicate keys, certificates, or their combination, for unauthorized identification of the user in the system. The malefactor undermines the work of the system, duplicating the identification data of other knots. Its purpose consists of mixing powers and to interfere with the identification of the participants of a road accident. This attack causes direct loss of data confidentiality and also of integrity, because the malefactor can redistribute the roles of the participants in the road accident in its own favor, if it implements it. The attack pursues the same aim, as well as aforementioned 'node impersonation', i.e. a violation of the AAA (Authentication, Authorization, Accounting) process of vehicles and transport infrastructure. Countermeasures include the creation of an information transfer secure channel; the use of keys with limited validity period, in order to avoid the use of a key by the malefactor, can be discussed.

3.7. Traffic Analysis—Definition of Topology of Network, Routing

The attack consists of the interception and different analysis of office and information packages which may contain data about location, identification, a route, etc. Such a passive attack allows the malefactor to be prepared for the realization of the powerful active attack. The analysis of traffic breaks the confidentiality of transfer of the message for all modes of exchange of OBU and RSU. This attack is aimed at a wireless network, because the network packages which are not intended for open access gather and are analyzed; the further direction of development of the attack is aimed at any ITS elements: on the vehicle and on transport infrastructure as along with the revealed network routes it is possible to organize the interception of packages of confidential information; and on wireless network for the organization of the effective DoS attack to which knowledge of its topology is considered the most important of conditions. Countermeasures include the creation of an information transfer secure channel.

3.8. Man in the Middle—Interception and Modification of Messages between Cars and Points of Access

This attack can be realized in two variations: one for the OBU mode and one for the RSU mode. In the first case, the knot of the malefactor (OBU) "listens" to the connection channel between other knots. In the case of RSU, the malefactor organizes an access point (transmitter) on the section of the road for interception (confidentiality violation) and modifications (violation of integrity) of messages; at the same time, the attacker's transmitter is connected to the main transmitter. Other knots are connected to the pseudo-transmitter, and transmit messages through it on the main transmitter; at the same time, the malefactor obtains all information going on the main transmitter from subscribers, as it was an unauthorized intermediary between them. This attack is aimed equally at the vehicle and at transport infrastructure, because both of these participants of the exchange "expect" that the opposite side is original, and transfer confidential information to it; actually the subscriber is the malefactor's knot.

Countermeasures include digital certificates in total with authentication methods and also hashing with keys.

3.9. Routing: Blackhole, Greyhole, Wormhole, Tunneling, etc.—Violation of a Data Route

This attack exploits the vulnerability of protocols of routing at the network level and has several versions. Blackhole is directed to the destruction of all packages which follow through the malefactor's knot; therefore, packages do not come to the recipient. Greyhole is directed to the destruction of only some part of packages, because it reduces the probability that the malefactor will be found by the next knots; other packages are broadcast correctly. All these attacks are directed at the violation of the integrity of networked data. Routing attacks are aimed at all elements of the intellectual transport system insofar as its functioning in general breaks. Therefore, the redirection of all traffic from transport on a knot of the malefactor will allow its confidential data to be received (after their interpretation), and the main exchange between knot and surrounding transport infrastructure to be stopped (to create effect of "a network shadow"). The establishment of an own routes of office VANET/ITS packages will allow not only the regular functioning of wireless network to be broken, but also subsequent attacks, such as DoS, to be mounted. Countermeasures were not found in the reviewed sources, however the use of the mechanism of the entrusted routing can be offered.

3.10. Global Positioning System (GPS) Spoofing/Hidden Vehicle (position faking)—Substitution of Coordinates of Knot Location

Using the Global Positioning System (GPS) simulator, the malefactor generates the signal, which surpasses in power a real signal of the satellite. Vehicles read out a stronger, false signal which broadcasts to the car the incorrect location taken for true. Hidden vehicle attack is a special case of a substitution of location data when the knot deliberately does not send the warning messages to another knot about the location of a road accident. Such attacks are directed to the violation of integrity of the messages sent by a knot with the location, as in the course of the attack these data are modified by the malefactor. The attack is aimed at the vehicle, providing incorrect information to it, which is obviously unsafe. For example, following the GPS navigator and accepting incorrect coordinates will at best not allow the destination to be reached in time, and at worst will lead to a road accident (for example, there will be no information on ongoing repair works, the road with oncoming traffic, abrupt turns, etc.). Countermeasures include the digital signature of data on a location can be recommended (the matter is under discussion in the scientific community, since a method of absolute elimination of this threat has not yet been determined).

The results of the analysis of the top 10 cyber threats for VANET/ITS regarding classification features and references are shown in Table 1, in which the following symbols are accepted: C—confidentiality; I—integrity; A—availability; V—the vehicle; TI—transport infrastructure; WN—wireless network.

Table 1. The list of "popular" cyber security threats to vehicle wireless networks.

Attack	Violation of Information Security: Immediate (mediate)	Target Object: Direct (indirect)	Wi-Fi	Cellular Communication
DoS (Denial of Service)	A	WN	[9–14]	[15–17]
Tracking	C	V	[10,12,18–27]	[28,29]
Routing	I	V, TI, WN	[10,30–32]	[15]
Tampering Hardware	C, I, A	V, TI	[8]	[15]
Sybil attack	(C), I, A	TI	[18,26,27,31,33–39]	
Traffic analysis	C	(V), (TI), WN	[10,19,25,40–43]	[15,44]
Jamming	A	V	[45]	[16]
Global Positioning System (GPS) spoofing/position faking	I	V	[11,20,31,46–53]	
Timing attack	C	WN	[12,14,31]	
Message tampering/suppression/fabrication	C, I	WN	[9,20,21,38,39,42,46,54–58]	[59–61]
Man in the middle	C, I	V, TI	[14,31,46,55,62]	[63,64]
Brute force	C	(V), (TI), WN	[26,32,65]	
Broadcast tampering	A	WN	[8]	
Node impersonation	C, I	V, TI	[10,20,24,26,34,36,55]	[15,66,67]
Replay	C	WN	[10,20,38]	[68]
Illusion attack	I	V, TI	[11,20,46]	
Key and/or certificate replication	C, I	V, TI	[12,18,26,35,54,69]	[37,70–72]
Malware Spamming	C, I	WN	[36]	[15,73]
Loss of event traceability	I, A	TI	[31,36,54]	

From Table 1 it can be seen that, in spite of the abundance of threats, practically all of them are characteristic of any wireless network; for VANET/ITS-specific threats, it is possible to carry out, perhaps, only GPS spoofing/position faking. The distinction of cyber threats for VANET/ITS, in case of its realization with the use of Wi-Fi or cellular communication, is distinctly shown, despite strong convergence.

Additionally, the malefactors-exploited vulnerabilities, which are the most important factor of generation requirements to protective measures, are not specified for all threats in the analyzed sources; at the same time, the level of these vulnerabilities—low to medium or high level—is not specified (architectural).

The last circumstance is critical for the further promotion of the concept of VANET/ITS, and the modification of its architectural model can be required in case of the detection of high-level vulnerabilities [78].

Table 2, presented in the form of a matrix with the measurements "Target Object vs. Violation of Information Security", represents the next and one of the many cyber threats taxonomy for VANET/ITS.

Creating such a taxonomy allows providing targeted research of VANET/ITS protection issues, in particular, to structure statistical data on cyber attacks, to highlight typical attack patterns (for example, attacks on WN that damage integrity), and to draw conclusions based on the collected data. Use of other classification criteria (for example: level of vulnerabilities (low, medium, high), potential violators (external, internal), etc.) leads to a systematic expansion of knowledge in the field of cyber resilience.

Table 2. Cyber threats taxonomy for vehicular ad hoc networks/intelligent transportation systems (VANET/ITS).

Direct Target Object	Immediate Violation of Information Security		
	Confidentiality (C)	**Integrity (I)**	**Availability (A)**
Vehicle (V)	• **Tracking**; • Tampering hardware; • **Man in the middle**; • **Node impersonation**; • **Key and/or certificate replication**	• **Routing**; • Tampering hardware; • **GPS spoofing/position faking**; • **Man in the middle**; • **Node impersonation**; • Illusion attack; • **Key and/or certificate replication**	• Tampering hardware; • Jamming
Transport Infrastructure (TI)	• Tampering hardware; • **Man in the middle**; • **Node impersonation**; • **Key and/or certificate replication**	• **Routing**; • Tampering hardware; • **Sybil attack**; • **Man in the middle**; • **Node impersonation**; • Illusion attack; • **Key and/or certificate replication**; • Loss of event traceability	• Tampering hardware; • **Sybil attack**; • Loss of event traceability
Wireless Network (WN)	• **Traffic analysis**; • Timing attack; • **Message tampering/ suppression/fabrication**; • Brute force; • Replay; • Malware spamming	• Broadcast tampering; • **Routing**; • **Message tampering/ suppression/fabrication**; • Malware spamming	• **DoS** (Denial of Service)

4. Risk Analysis

The process of determining cyber threats, vulnerabilities and potential damage belongs to the field of knowledge called risk analysis and it is one of the most complex and important in predicting the cyber-resistance of VANET/ITS. The definition of cyber threat involves identifying it, which was practically addressed above for the top 10 threats except of the type and potential of the malefactor, i.e. source of threat. Opportunities of the violator that are sufficient for the implementation of cyber threats to VANET/ITS are undoubtedly a special topic of study but are not critical for the further presentation of the problematic issues in the prediction of its cyber resistance.

An identified cyber threat may have some risks and it is subject for neutralization (blocking) if it is relevant to VANET/ITS. Cyber threats are relevant for VANET/ITS with given structural and functional characteristics and functioning features if there is a likelihood of the cyber threat probability being actualized by the malefactor with the corresponding potential and its implementation will lead to unacceptable negative consequences (damage) from breach of confidentiality, integrity or availability of information.

As an indicator of the j-th cyber threat (A) relevance, a vector can be used, the first component of which characterizes the likelihood of the threat (Pj), and the second—the degree of possible damage in case of its realization (Xj). Traditionally, Pj is determined on the basis of statistical data analysis on the frequency of cyber threats in an information system and (or) similar information systems, and Xj is defined based on an assessment of the degree of confidentiality breach consequences, integrity or availability of information.

In the absence of statistics on the occurrence of security incidents, which is typical of VANET/ITS as an innovative cyber system, the relevance of cyber threats will be determined based on an assessment of the cyber threats (Yj) possibility. Yj will be determined based on an assessment of the level of the system security and the potential of the malefactor required to implement cyber threats. Such an assessment today is carried out in the overwhelming majority of cases by an expert method and it is predictive in relation to cyber resilience (will be discussed below).

5. Synergetic Approach

It follows from Item 2 that questions of cyber security of 802.11p and LTE-V are already quite well researched, as today there are only individual publications that are devoted to their safe joint functioning [79,80]. The complexity of researching this issue arises from a new communication mix (so called "hybrid"). As this hybrid is the result of sharing DSRC/802.11 and LTE-V, from the point of view of cyber security it represents another essence, which is different from the parts forming it, when their vulnerabilities form the effect of synergy.

This synergy is formed due to the operation of the following mechanisms. Firstly, some properties of the first part of the communication mix (for example, DSRC/802.11p) can serve as neutralizing measures for cyber threats of the second part (for example, LTE-V), and vice versa. Secondly, other properties of the first part can represent sources of threats for the second part, and vice versa. Thirdly, similar vulnerabilities can reinforce each other and initiate fatal cyber threats.

The resulting cyber resilience of "hybrid" of VANET/ITS does not come down to the simple sum of the cyber resilience of its components (DSRC/802.11p and LTE-V) in any cases.

If the resulting cyber resilience of "hybrid" is lower than the components, then their association has to be recognized as unsafe. The cyber threats which have remained and appeared in "hybrid" have to be compared with its vulnerabilities. As a result, preventive measures can be used concerning the predicted vulnerabilities, because the latter became known before the current incidents of cyber security.

The analysis of Tables 1 and 2 shows the existence of a difficult dependence of total cyber resilience of VANET on the ITS telecommunication component, from cyber threats to the applied wireless technology.

In the case of the hybrid option, the situation often becomes complicated due to presence of synergetic effects. To provide harmonious and effective existence of "communication mix", a certain supervising program will be required, which is capable of exchanging the level of cyber security of critical applications for functional requirements of ITS regarding reliability of reception/transfer, the maximum delay of messages, and other probabilistic and time characteristics, situationally (depending on the road and other milieu).

Employing software-defined networking (SDN) technology can be one such decision. This technology is based on the principle of division according to the planes of management and data, and this situation hypothetically allows realizing the above-stated exchange [81,82].

In this case, the conceptual VANET/ITS model can be considered as a new cyber essence, software-defined internet of vehicles (SDIoV), formed by the certain "automobile world" of the internet of things (IoT) (the so-called internet of vehicles, IoV) in the form of a set of terminal device sensors which are built into vehicles and physical infrastructure facilities and generate problem-oriented traffic, on the one hand, and the SDN technology applying for the solution of problems of its cyber-stable service, on the other. However, both SDN and IoV cannot be considered ideal from a position of cyber security, as besides the new advantages they bring they are also associated with certain cyber threats, which are a consequence of vulnerabilities of their own architectural concepts [78] and technical realization.

The declared synergetic approach can be shown as a step-by-step algorithm in relation to a qualitative assessment task of cyber resilience of SDIoV and forecasting its vulnerabilities as follows.

Step 1: To reveal a set of the cyber threats which are traditionally initiated by architectural vulnerabilities of SDN and IoV. For this purpose, it is possible to use a pool of the publications devoted to the safety of IoT (IoV) and SDN, including the report of the international open consortium OWASP [83].

Step 2: To estimate possibilities of neutralization of cyber threats of SDN, of advantages of the use of IoV, and to establish the vulnerabilities of SDN which have lost relevance for SDIoV. To make asymmetric operations: to estimate possibilities of neutralization of cyber threats of IoV by advantages of the use of SDN and to establish the lost vulnerabilities of IoV.

Step 3: To estimate possibilities of transformation of architectural features of SDN into sources of cyber threats for IoV, to establish the new vulnerabilities exploited by them, and to make asymmetric operation for architectural features of IoV.

Step 4: To compare cyber threats of the united parts on a similarity subject. If in the SDIoV system two similar cyber threats from SDN and IoV are defined, then this threat appears in both parts of the system and cannot be essentially neutralized by them. It is furthermore necessary to establish the architectural vulnerabilities of SDN and IoV initiating it.

As a result of performing Steps 2–4 of the algorithm on a set of the cyber threats and vulnerabilities revealed in Step 1, it is possible to forecast vulnerabilities for SDIoV. We will predict vulnerabilities of SDIoV for cases of operation of all three synergetic mechanisms—neutralizations (N-effect, Neutralization), generation (G-effect, Generation), and reinforcement (I-effect, Interference).

One implementation of the concept of IoV are wireless touch networks. Because of their small size and spatial distribution, the IoV devices energy supply can be carried out at the expense of non-renewable power sources with a limited charge; the latter defines a new cyber threat for IoV applications, namely attack implementation on a power system of a touch network for the purpose of 'harvesting' energy from its knots [84].

5.1. Case 1: Low Power Consumption of Sensor Network Knots

With this purpose, malefactors can use streams of false events, because the false event (for example, inquiry) as well as being legal, surely provokes reaction of a touch knot which demands additional power consumption and "exhausts" it, thereby reducing the life cycle of IoV network. At the same time, SDN allows the centralized management of data flows, and besides is not dependent on the number of the devices generating the last ones. Streams concerning devices can be both regarded as input/output, but in the context of the considered threat we are interested in the former. Thus, one correction of the network activity of devices is possible according to the set purpose—the restriction of the number of office packages in the network. As a result, IoV devices save scarce energy, and their low power consumption stops being a critical vulnerability.

The basic possibility of the centralized management of data flows, inherent to SDN, is capable of neutralizing one more vulnerability of IoV.

5.2. Case 1: Possibility of Cloning Packages

One of the cyber threats to the "microcosm" is connected with a practical lack of sufficient computing opportunities for IoV devices that necessitates the request for computational power from the "cloud" service. It has been experimentally proved [85] that on all routes of data from the IoV device to a cloud service there can be a destruction, distortion, and blocking of the transmitted data. A special type of cyber attack is the transportation (or duplication) of IoV traffic at the expense of cloning of network packages in the false cloud IoV server. The noted possibility of SDN of the centralized control of routes of IoV traffic makes package cloning useless from the point of view of the malefactor. In such a way, because of merging with SDN, one more vulnerability of IoV will not be inherited by SDIoV.

The same architectural feature of SDN which in the previous case led to the neutralization of a number of vulnerabilities of IoV can serve as a vulnerability for SDIoV in another case.

5.3. Case 2: A Possibility of Purposeful Management of Network Traffic of a Set of Uncontrolled Devices

The concept of IoV offers the existence of the physical things comprising sources of network activity. The number of the latter tends to constantly grow, and their network distribution aspires to the organization in groups with weak differentiation. Thereby, the set of the chosen SDN and IoV properties (which are not separately expressed vulnerabilities) leads to the emergence of new vulnerability—a possibility of purposeful management of network traffic of a set of almost uncontrolled devices. The threat of carrying out the subsequent distributed DoS (DDoS) attack in this case can be realized in the two following ways: firstly, the organization of the purposeful attack to the same IoV devices (and therefore equally vulnerable) for their infection and the creation of the zombie network; secondly, direct redirection of valid traffic of IoV devices on the attacked knot. An opportunity for the operation of a vulnerability can be received by both the short-term "hacking" of the SDN controller by the malefactor, and the direct attraction of third-party IoV devices in SDN.

The SDIoV system received by the immersion of SDN technology to the IoV "world" will include the vulnerabilities that have reinforcing influence on total cyber resilience. We will consider the new received SDIoV system from this position.

5.4. Case 3: Absence of Control of Network Configuration

On the one hand, manual SDN control, at a rather weak automatic check of its accuracy, leads to the creation of a wrong configuration at the top level of the system. The threat of realization of this vulnerability can generally be weakened by automatic fine-tuning of lower knots of the network, for example, by preventing the usage of predicted unsafe network routes. On the other hand, mistakes in IoV configuration, having mass character, are capable of breaking the accuracy of network work at the lower level of a system. Control of such wrong work can be delegated to the controllers, which operate the general scheme of package transfer; for example, they can automatically construct a 'barrier' by the boundary devices of the network; they are interfering with the dissemination of confidential information out of the established zone.

Thus, during the work separately, on each level the application of specialized analysis algorithms and management will allow the partial or complete neutralization of configuration errors of other level. The joint use of SDN and IoV will introduce vulnerabilities of configuration in total SDIoV, which will not only be united, but are also strengthened (effect of an interference), because their exploitation will obviously become simpler. This is because the malefactor will take control of a uniform role in the system, which allows manual settings of a configuration SDIoV to be made.

We will estimate the received SDIoV from a cyber resilience position due to a potential success consideration of cyber attacks for vulnerabilities of various genesis [86].

The attempt of SDN and IoV vulnerability exploitation, which are neutralized partially or completely in a total SDIoV cyber system, will no longer result in essential damage, even with considerable variations of vector attack initial parameters. This is an obvious sign of cyber resilience.

Therefore, the realization of more effective management of network streams as reasonable mitigation of cyber threats will be more effective than fighting against low power consumption of a separate group of devices (Case 1) in a physical way (as, most likely, the malefactor for sufficient time is capable of practically discharging any independent IoV device)—in other words, management is better than attempting to create an idealized picture.

The reverse situation arises for the case of an interference of vulnerabilities from both parts of a cyber system, leading to SDIoV having the worst safety of each of the initial elements or even their sum. However, the realization of the protective measures directed to neutralize the total vulnerability can potentially lead to an increase of indicator of cyber resilience, for the reasons, similar to the previous case, that separate vulnerabilities in the system will be present, and the threat from the exploitation of everyone (as well as their sums) will be minimized. Therefore, it makes sense not to create separate instruments of automatic checking of configurations of each system level (Case 3), but rather to provide control access to configuration files and to increase the qualification of administrators; otherwise, random errors in check instruments, as well as malicious logic, will nullify all attempts to ensure perfect automatic protection against the wrong settings.

The cyber resilience indicator of a final system behaves differently in terms of generating new vulnerabilities there. It is obvious that the general safety of such cyber systems will be considerably reduced, which will prevail over its opportunity to adapt to cyber attacks; at least, the process of evolution to the required level will be rather strongly dragged out in time. For instance, the possibility of the DDoS attack implementation by the malefactor with attraction of legal IoV devices (Case 2) can in theory be neutralized by the creation of the relevant legal framework, but the real effect of such base will not be visible soon enough. At the same time, a more mobile system of DDoS attack construction by the malefactor at the expense of time for adaptation itself will have a cyber resilience property to neutralized measures.

6. Top 10 SDIoV Cyber Threats

We will apply the offered algorithm regarding the forecasting of the cyber resilience of SDN and IoV in the case of their joint functioning within SDIoV.

The analysis of publications [87–91] concerning the cyber security of SDN has allowed the allocation of the top 10 threats generated by its vulnerabilities. The results of this qualitative analysis, according to Step 2 of the algorithm, are given in Table 3.

Table 3. Results of synergetic impact of the internet of vehicles (IoV) on the vulnerabilities of software defined networking (SDN).

SDN threat	SDN vulnerability	Synergetic impact of IoV
SDN_01: Using unauthorized controllers	Architectural feature of SDN is allocation of the module of management in a separate element of system—the controller. Therefore, unauthorized access to the controller will lead to the violation of functioning of the network or to complete malefactor control.	None
SDN_02: Using unauthorized applications	The logic of operation of the SDN controller is adjusted at a higher level, exactly in applications. Thus, unauthorized access to the application will lead to a threat that is similar to SDN_01 consequences.	None
SDN_03: Account) data leak	Interception of the packages by the malefactor that are sent to the controller will allow their analysis, that can subsequently be used for the intentional generation of wrong packages. Certificates and keys (account data) can also be intercepted by the malefactor, which is inadmissible.	Formation of I-effect with IoV_02 is possible (see Table 4).
SDN_04: Data modification	The scheme of the wireless network built on the principles of SDN is vulnerable to "man in the middle" type attacks.	Formation of N-effect is possible: The development of special protocols of exchange for IoV devices will allow the reduction of the risk of modification of data or finding the fact of such modification.
SDN_05: Denial of service	Features of processing of new streams in SDN can potentially lead to denial of service (DoS) attack implementation.	Formation of N-effect is possible: Protocols for IoV devices can be adjusted in such a way to minimize traffic and to reduce the risk of implementation of a DoS attack.
SDN_06: Misconfiguration and human factor	The wrong configuration of devices influencing safety of all SDN levels represents a typical and rather serious threat for any network. The possibility of manual control of a configuration on the part of the client automatically leads to the threat of a so-called "human factor".	Formation of I-effect with IoV_10 is possible (see Table 4); it is considered above (see Case 3).
SDN_07: Creation of unencrypted network channels	The lack of the mandatory requirement to use transport layer security (TLS) in the OpenFlow protocol is going to be threat of cyber security of SDN, being a consequence of its architecture.	None
SDN_08: Inner protocol network elements	The SDN model allows short-term interruptions of network connections. The detection of the loss of connections by the controller at the same time will not be instant, which will finally lead to a loss of data.	Formation of I-effect with IoV_04 is possible (see Table 4).
SDN_09: OpenFlow usage	The absence in OpenFlow of "clever switching" together with sending the special teams by the malefactor to devices supporting OpenFlow can lead to the violation of work of stand-alone programs (applications) or of the whole network.	None
SDN_10: API layer interaction	One more weak point in the architecture of SDN is the interface of the interaction of applications, controllers and routers, leading to corresponding threats.	None

The results of the similar procedure for IoV (based on [92–96]) are shown in Table 4.

Table 4. Results of synergetic impact of SDN on vulnerabilities of IoV.

IoV threat	IoV vulnerability	Synergetic impact of SDN
IoV _01: Public IP hacking	Presence of open and insecure IP; this applies to the majority of IoV devices, and allows the implementation of the corresponding attacks, which causes the system to break.	Formation of N-effect is possible: The correct organization of SDN streams minimizes or limits access for the malefactor to IoV devices with public IP.
IoV _02: WLAN link interception	Interception of open traffic of IoV devices by WLAN allows the malefactor to obtain confidential information, using which they are able to carry out subsequent attacks.	Formation of I-effect with SDN_03 is possible (see Table 3).
IoV _03: "Brute-force" attack	Access to control of IoV devices can be provided by brute force attack on an account's password, because of the lack of a serious system of authentication in the case of their weak computing power.	None
IoV _04: Cloud connection halting	Even short-term failure of the exchange of traffic of IoV devices with a cloud can lead to the full infrastructure's refusal.	Formation of I-effect with SDN_08 is possible (see Table 3).
IoV _05: Destructive electromagnetic influence	Weak signals from IoV devices can be lost in the case of influence by a close or purposeful electromagnetic impulse.	None
IoV _06: Fake connecting	The IPv6 mechanism, used for IoV network scaling, allows the malefactor to create fake IoV devices, redirecting necessary traffic on itself.	Formation of N-effect is possible: The SDN controller can partially operate streams at the time of addition of the new IoV device; this means "false" knots cannot connect to a network (including to "clouds"). This is considered above (see Case 1*).
IoV _07: Physical access	The main feature of IoV devices is their very small size, and the possibility of embedding in household objects is a serious threat in the case of a malefactor's physical access to them.	None
IoV _08: Energy depletion	The very small sizes of IoV devices require them to use batteries (because of the lack of a strict main power feed) with a limited validity period. This period of time can be considerably reduced by the malefactor by the creation of operating conditions of the IoV device with excessively high loading.	Formation of N-effect is possible: The ability of SDN and algorithms of operation of its controller to trace network loading allow the prevention of the exhaustion of energy of IoV devices; it is considered above (see Case 1).
IoV _09: Buggs	The vulnerabilities that are present at any difficult software can often be destructive for IoV networks.	None
IoV _10: Error clone	Mass setup of the same IoV devices leads to the duplication of a wrong configuration.	Formation of I-effect with SDN_06 is possible (see Table 3); it is considered above (see Case 3).

A concept scheme of the process of synergetic impact of SDN on vulnerabilities of IoV (and vice versa) under the new cyber essence (SDIoV) is presented in Figure 1.

The qualitative analysis of the contents of Tables 3 and 4 allows it to predict that from the top 10 cyber threats of SDN can be neutralized only two of them by synergy of IoV (N-effect). Respectively, only three for IoV due to SDN. That is, the majority of threats to SDN and IoV in SDIoV will remain, and some of them will even be amplified (I-effect). Taking into account this circumstance, and the inevitable initiation of new cyber threats (G-effect), it is expedient to expand SDIoV by a new component which is a specialized subsystem of ensuring cyber security.

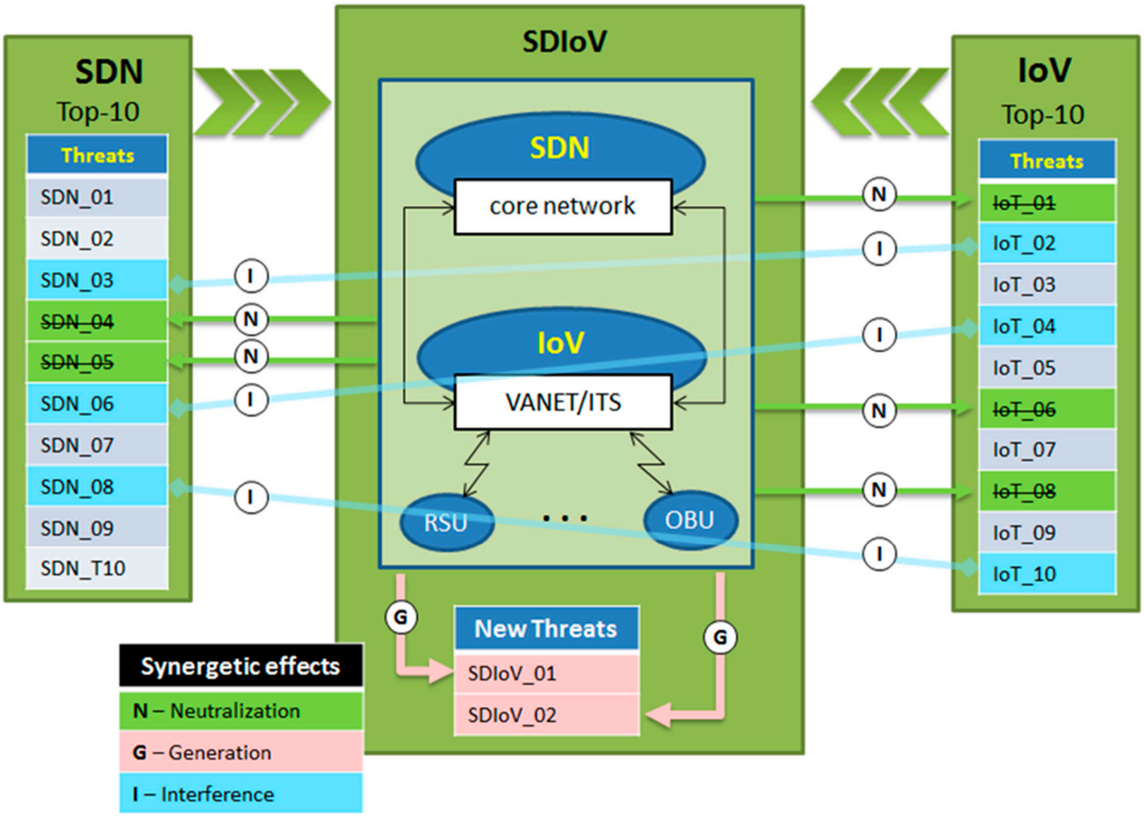

Figure 1. A concept scheme of the process of synergetic influence in SDIoV.

7. Expert Forecasting Cyber Resilience of Variants of Creating VANET/ITS

In the application of the described synergetic approach, even for the qualitative assessment of cyber resilience of "hybrid" of VANET/ITS and forecasting its vulnerabilities, there are essential restrictions.

Firstly, this study only considers the combination of two technologies, DSRC/802.11p and LTE-V, although in reality the synthesis of new cyber systems from the whole cascade of technologies "full hybrid communication mix" type can be required [4]. Secondly, it is considered that in a new cyber system the condition of vulnerability is static; it can only disappear, arise or be transformed to another one. Real vulnerabilities have dynamic properties and are capable of continuing modification throughout the life cycle of cyber systems and under the influence of external factors; thus, the description of the subsequent states requires the use of more difficult scientific approaches and methods. Thirdly, the forecasting of a new cyber system (for example, "hybrid") is based in the assumption that its development is determined. The indisputable complexity of the majority of cyber systems (which are practically all in the sphere of communication technologies and safety) demands the consideration of the processes related to them as stochastic, i.e., developing on various ways with various probabilities.

Nevertheless, even taking into account all sufficiently essential restrictions of a definite answer (at least qualitative, not to mention the calculation of any quantitative measures) it is not possible to receive. Therefore, in VANET/ITS, the existing vulnerabilities can disappear, appear again or become amplified; some of these will lead to the strengthening of cyber resilience, and some will have the opposite effect.

The main reason for such uncertainty is that the existing methodology and the tools serving information security do not allow the forecasting of a condition of difficult cyber systems, in feature applicable in practice, i.e., having the sufficient level of pragmatism.

For such a case, one of the only ways of forecasting is to use up-to-date expert estimates.

As tools, the hierarchy analysis method of Saati [97] (conditionally the first method) in combination with a sampling method (conditionally the second method) is considered by authors.

The first method includes procedures of synthesis and the analysis of multiple judgments of experts concerning the priority of indicators and the choice of rational options among alternatives. As alternatives, the options of development VANET/ITS considered in Chapter 1 can act here: the "standardized" VANET (DSRC/802.11p), "mobile" VANET (LTE-V), and "hybrid".

All of the aforementioned alternatives rely in the majority of cases on modern wireless technologies, but at the same time they have specifics in the organization of communications within the implementation of the aforementioned concept.

Indicators describing the most essential properties of alternative information and telecommunication systems, and changing the values in time, can be, for example: a cyber security vector as a part of indicators of confidentiality, integrity, availability, and non-repudiation; and productivity vector as a part of indicators of throughput ability, multi-service and timeliness. The offered indicators are interconnected; for example, requirements to timeliness characterize availability, etc. Therefore, the created generalized criterion of estimation of cyber resilience of ITS telecommunication component considered essential internal properties of a cyber system can be presented in the form of joint conditional probability of implementation of requirements for cyber security and productivity.

The second method includes statistical research of the general properties of objects (alternatives) on the basis of the studying of the properties only of the sample.

The judgments received by the first method are static, and their values do not allow solving a problem of forecasting, because its decision is based on the dynamic change of priorities. The analytical solution of the specified task is in [98], where for receiving estimates of coordinates of an own vector the sampling method is used.

The received indicators represent continuous differentiated functions of time. Therefore, it is possible to execute the differentiation of these functions to define growth rates of the studied priorities. Dependences on the change of priority growth rates for three alternative options of the organization of VANET/ITS communications obtained by authors show that the rate of change of a priority, which is a defining property of cyber security for the first alternative (DSRC/802.11p), is negative. Its biggest absolute value is predicted in the first years, and after that this value decreases.

Priorities change tempo and are approximately identical to those of the two other alternative options.

The paired relations of the received similar derivatives have allowed the comparison of growth rates of the extent of realization of each property for the considered alternatives. This study shows that the rate of change of the property of cyber security for the second alternative, LTE-V, is highest in the first years, which represents the greatest efficiency of its implementation in the nearest future. In prospect, the effect of its implementation in comparison with other alternatives falls. In the medium-term and long-term forecast, it is expedient to develop the third alternative, "hybrid", that does not contradict global trends.

8. Challenges

Taking into account the above, we summarize the aforementioned problematic issues of the cyber resilience telecommunication component of intelligent transportation systems.

Issue 1: Classification vs. terminology. In spite of the significant amount of publications about the threats of cyber security in VANET networks, these generally involve surveys or grouping of classical features for telecommunication networks.

This means that incorrect classification features are used; they do not take into consideration specifics of vehicle wireless networks.

The reason for such a situation, in our opinion, is the insufficient base preparation of modern writers in the cyber security sphere. This happens because they are keen on "best practice", which is detriment for theoretical and methodological preparation.

For the same reason, a serious problem for systematization (and the subsequent successful classification) is also terminological confusion leading to the shift and mixture of the terms "vulnerability", "threat source", "damage", "attack", and "threat". On the other hand, classification of threats of cyber resilience of VANET is an uncommon task even for "classical scientists", in view of its complexity as an object of study, because it is not a just a specific segment of a wireless network, but rather a set of dissimilar devices; each threat has to be specified from a position of a possibility of its realization in relation to a concrete layer of ITS, e.g., OBU, RSU, V2V, V2I, etc.

Issue 2: Space vs. time. Investigating the genesis of cyber resilience of VANET/ITS, this study has established that the main source of threats for cyber systems is the high-level (architectural) vulnerabilities of its components.

These are generated by features of realization of some conceptual model, and most actively participate in synergetic effects. In view of the above, such analysis requires special conditions such as spatial taxonomy (stratification) of vulnerabilities, at least for the high, medium, and low levels. Any mechanisms for the development of vulnerabilities, even for the simplest cyber systems in time (such as evolution, revolution, coevolution, etc.), are also almost disregarded. Therefore, it is necessary to recognize the VANET/ITS phenomenon as relevant. On the one hand, such an infocommunication system inherits the vulnerabilities of its parts, and on the another hand develops essentially new vulnerabilities [99].

Issue 3: Productivity vs. cyber security. This issue, mentioned before (see Item 3), assumes the situational exchange of productivity on the cyber security of VANET/ITS, and vice versa for the benefit of the maintenance of the required level of its cyber resilience. The mechanism of such exchange has been the focus of limited study. The attempt made in this study to use SDN technology as some regulator ("solver") transforms this issue to the plane of a problem of the optimum (rational) choice of the level of centralization of network management, even up to the realization of completely decentralized VANET [100].

Issue 4: Forecasting vs. "best practice". It is necessary to recognize forecasting in the field of cyber resilience research, such as priority direction, because it is aimed at the prevention of destructive consequences. At the same time, this direction is mostly "a weak link" for the aforementioned reasons. The lack of representative "best practice" prevents an opportunity to use the predictive power of classical mathematics, inevitably leading to expert estimation, and has trend to "a human factor", e.g., unreliability, limitation, engagement, etc.

The authors believe that implementing the following steps, which can help to solve the problem of formulated collisions and scientific knowledge gaps (directed to solve this collisions) in the future, provides an opportunity for the creation of missing scientific, theoretical, and methodological bases for comprehensive descriptions and solutions for the issue of critical questions of assessment, forecasting, and providing cyber resilience to all kinds (and complexities) of systems.

At first, the formalized establishment of the fundamental concepts, such as vulnerability and cyber threat will be needed, which will allow all facts to be accumulated methodically, and have a true cyber security (cyber resilience) research 'landscape'.

Secondly, properties of the central cyber security object—vulnerability—should be deeply analyzed. We mention not only static characteristics, but also dynamic ones, because they have a higher priority. Forecasting the security of a new cyber system is basically impossible without dynamic characteristics. Thirdly, specialized mathematics is needed to comply with the rigidity of scientific judgement. Such a set of mathematical tools includes the notation of description of system state from the point of view of cyber security, and also algorithms, which connect the states according to current synergetic mechanisms. Fourthly, the problem of balance between productivity and security should be stated in terms of degrees of centralization and levels of cyber system management. Finally, the practical use of the developed scientific and methodological base will require the development of problem-oriented software solutions allowing the modeling of development processes of cyber systems to estimate their parameters and to forecast vulnerabilities.

9. Conclusions

The authors analyzed the paradoxical situation of intelligent transportation systems in the field of information security, which consists of a sharp "surge" of identified threats (including zero-day) for a not yet completely formed, practically new cyber system, in order to identify problematic issues of forecasting cyber resistance of its connected components based on wireless technology.

There are 3 main options for constructing cyber-resilience telecommunication components for intelligent transportation system from sustainable global trends: "standardized" (DSRC/802.11p), "mobile" (LTE-V) and their "communication mix" are allocated.

The authors detail a set of the known threats of cyber security in wireless automobile networks according to the initial scheme: the attack mechanism–the exploited vulnerability–information security damage–object of attack–a countermeasure.

As an object of attack, it was proposed to consider the three main elements of an intelligent transport system: vehicles, transport infrastructure and wireless information and technical interaction between them.

The authors used the effects of the synergistic approach they established to qualitatively assess the cumulative effect of combining various cyber systems concepts. As an example, a qualitative prediction of cyber resilience of a certain new entity formed by the merger of a software-configured network and the "automotive" internet of things has been proposed.

The solution of the quantitative forecasting problem of the wireless automotive networks cybersecurity in the article is to establish on a change in the values of global priorities when comparing alternative options for organizing information technology interaction. As a toolkit, it was proposed to use the T. Saaty hierarchy analysis method in combination with the sampling method, and as alternatives, formed variants of a coherent component of an intelligent transport system.

As a result, the problem questions for predicting the cyber-resilience of the intelligent transport system coherent component are formulated. A sequence of steps is proposed to resolve the formulated collisions by creating the missing scientific (theoretical and methodological) and instrumental basis.

The authors are aware of the incompleteness of the described problematic issues list in predicting the cyber resilience of VANET/ITS, caused by the limited scope of the article. Left out of consideration were important issues; for example, the problem of deploying a general trust model [101] between the main subjects of ITS (terminals, applications etc.) based on public key infrastructure. Also, there is a problem of technical, informational and organizational compatibility of 'communication mix', i.e., the ability of a coherent component to exist on the basis of conflict-free and harmonious interaction of various telecommunication technologies. However, the steps proposed above will allow us to move from solving delayed issues of exploited vulnerabilities from practical neutralization to preventive tasks of modeling, forecasting and designing cyber systems like VANET/ITS with a given level of cyber resistance [102].

Author Contributions: All authors contributed equally to this work.

Funding: This research was funded by the Ministry of Education and Science of the Russian Federation in the framework of the Federal Target Program "Research and development on priority directions of scientific technological complex of Russia for 2014–2020" (agreement number 14.604.21.0165, unique identifier project RFMEFI60417X0165).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lu, M. *Evaluation of Intelligent Road Transport Systems: Methods and Results*; IET: London, UK, 2016.
2. Zubedi, A.; Jianqiu, Z.; Arain, Q.A.; Memon, I.; Khan, S.; Khan, M.S.; Zhang, Y. Sustaining Low-Carbon Emission Development: An Energy Efficient Transportation Plan for CPEC. *J. Inf. Process. Syst.* **2018**, *14*, 322–345.

3. Ahmad, F.; Adnane, A.; Franqueira, N.L. A Systematic Approach for Cyber Security in Vehicular Networks. *J. Comput. Commun.* **2016**, *4*, 38–62. [CrossRef]
4. Wevers, K.; Lu, M. V2X Communication for ITS—From IEEE 802.11p Towards 5G. *IEEE 5G Tech. Focus* **2017**, *1*. Available online: https://5g.ieee.org/tech-focus/march-2017/v2x-communication-for-its (accessed on 31 August 2018).
5. Federal Motor Vehicle Safety Standards; V2V Communications. Docket No. NHTSA-2016-0126. Proposed Rule. *Federal Regist.* **2017**, *82*, 3854–4019. Available online: https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf (accessed on 31 August 2018).
6. Filippi, A.; Moerman, K.; Martinez, V.; Turley, A.; Haran, O.; Toledano, R. *IEEE802.11p Ahead of LTE-V2V for Safety Applications*; Autotalks: Netanya, Israel, 2017; Available online: https://www.auto-talks.com/wp-content/uploads/2017/09/Whitepaper-LTE-V2V-USletter-05.pdf (accessed on 31 August 2018).
7. Festag, A. Standards for Vehicular Communication—From IEEE 802.11p to 5G. *Elektrotech. Inftech.* **2015**, *132*, 409–416. [CrossRef]
8. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet Security Challenges and Solutions: A Survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
9. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]
10. Raw, R.S.; Kumar, M.; Singh, N. Security Challenges, Issues and Their Solutions for VANET. *Int. J. Netw. Secur. Its Appl.* **2013**, *5*, 95–105. [CrossRef]
11. He, L.; Zhu, W.T. Mitigating DoS Attacks Against Signature-Based Authentication in VANETs. In Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; Volume 3, pp. 261–265. [CrossRef]
12. Raya, M.; Hubaux, J.P. The Security of Vehicular Ad Hoc Networks. In Proceedings of the 3rd ACM workshop on Security of Ad Hoc and Sensor Networks (SASN'05), Alexandria, VA, USA, 7–10 November 2005; pp. 11–21. [CrossRef]
13. Hasrouny, H.; Bassil, C.; Samhat, A.; Laouiti, A. Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET. *Adv. Intell. Syst. Comput.* **2017**, *548*, 71–83. [CrossRef]
14. Chuang, M.C.; Lee, J.F. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks. *IEEE Syst. J.* **2014**, *8*, 749–758. [CrossRef]
15. Macaulay, T. *The 7 Deadly Threats to 4G*; McAfee: Santa Clara, CA, USA, 2013.
16. Mpitziopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A Survey on Jamming Attacks and Countermeasures in WSNs. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 42–56. [CrossRef]
17. Ma, D.; Tsudik, G. Security and Privacy in Emerging Wireless Networks. *IEEE Wirel. Commun.* **2010**, *17*, 12–21. [CrossRef]
18. Samara, G.; Al-Salihy, W.A.H.; Sures, R. Security Analysis of Vehicular Ad Hoc Networks (VANET). In Proceedings of the Second International Conference on Network Applications Protocols and Services (NETAPPS), Kedah, Malaysia, 22–23 September 2010; pp. 55–60. [CrossRef]
19. Whyte, W.; Weimerskirch, A.; Kumar, V.; Hehn, T. A Security credential management system for V2V communications. In Proceedings of the IEEE Vehicular Networking Conference (VNC), Boston, MA, USA, 16–18 December 2013; pp. 1–8. [CrossRef]
20. Intelligent Transport Systems (ITS); Security. *Threat, Vulnerability and Risk Analysis (TVRA)*; ETSI TR 102 893 V1.1.1 (2010-03); ETSI: Sophia Antipolis, France, 2010.
21. Guo, J.; Baugh, J.P.; Wang, S. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. In Proceedings of the 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 11 May 2007; pp. 103–108. [CrossRef]
22. Salem, F.M.; Ibrahim, M.H.; Ibrahim, I.I. Non-Interactive Authentication Scheme Providing Privacy among Drivers in Vehicle-to-Vehicle Networks. In Proceedings of the 2010 Sixth International Conference on Networking and Services, Cancun, Mexico, 7–13 March 2010; pp. 156–161. [CrossRef]
23. Intelligent Transport Systems (ITS); Security. *Trust and Privacy Management*; ETSI TS 102 941 V1.1.1 (2012-06); ETSI: Sophia Antipolis, France, 2012.
24. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET Security Surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]

25. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and Robust Pseudonymous Authentication in VANET. In Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET '07), Montreal, QC, Canada, 10 September 2007; pp. 19–28. [CrossRef]
26. Raya, M.; Papadimitratos, P.; Hubaux, J.P. Securing Vehicular Communications. *IEEE Wirel. Commun.* **2006**, *13*, 8–15. [CrossRef]
27. Xiao, B.; Yu, B.; Gao, C. Detection and Localization of Sybil Nodes in VANETs. In Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06), Los Angeles, CA, USA, 26 September 2006; pp. 1–8. [CrossRef]
28. Ohigashi, T.; Morii, M. A practical message falsification attack on WPA. In Proceedings of the Fourth Joint Workshop on Information Security (JWIS 2009), Kaohsiung, Taiwan, 6–7 August 2009.
29. Christof, P.; Pelzl, J.; Preneel, B. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer: Berlin, Germany, 2010.
30. Rawat, A.; Sharma, S.; Sushil, R. VANET: Security Attacks and Its Possible Solutions. *J. Inf. Oper. Manag.* **2012**, *3*, 301–304.
31. Vinh, H.L.; Cavalli, A.R. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. *Int. J. Ad Hoc Netw. Syst.* **2014**, *4*, 1–20. [CrossRef]
32. Patel, N.; Jhaveri, R.H. Trust Based Approaches for Secure Routing in VANET: A Survey. *Procedia Comput. Sci.* **2015**, *45*, 592–601. [CrossRef]
33. Van der Heijden, R. Security Architectures in V2V and V2I Communication. In Proceedings of the 13th Twente Student Conference on IT, Enschede, The Netherlands, 21 June 2010.
34. Al-Kahtani, M.S. Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs). In Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 12–14 December 2012; pp. 1–9. [CrossRef]
35. Rao, A.; Sangwan, A.; Kherani, A.A.; Varghese, A.; Bellur, B.; Shorey, R. Secure V2V Communication with Certificate Revocations. In Proceedings of the Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 11 May 2007; pp. 127–132. [CrossRef]
36. Singelee, D.; Preneel, B. Location verification using secure distance bounding protocols. In Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, Washington, DC, USA, 7–10 November 2005; pp. 834–840. [CrossRef]
37. Zhou, T.; Choudhury, R.R.; Ning, P.; Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 582–594. [CrossRef]
38. Yan, G.; Olaruis, S.; Weigle, M. Use of Infrastructure in VANETs. *Comput. Commun.* **2008**, *31*, 2883–2897. [CrossRef]
39. Kushwaha, D.; Shukla, P.K.; Baraskar, R. A Survey on Sybil Attack in Vehicular Ad-hoc Network. *Int. J. Comput. Appl.* **2014**, *98*, 31–36. [CrossRef]
40. Ploößl, K.; Federrath, H. A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks. *Comput. Stand. Interfaces* **2008**, *30*, 390–397. [CrossRef]
41. Abuelela, M.; Olariu, S.; Ibrahim, K. A Secure and Privacy Aware Data Dissemination for the Notification of Traffic Incidents. In Proceedings of the VTC Spring 2009—IEEE 69th Vehicular Technology Conference, Barcelona, Spain, 26–29 April 2009; pp. 1–5. [CrossRef]
42. Raya, M.; Aziz, A.; Hubaux, J.P. Efficient Secure Aggregation in VANETs. In Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET '06), Los Angeles, CA, USA, 24–29 September 2006; pp. 67–75. [CrossRef]
43. Mousumi, P.; Gautam, S. Traffic Analysis of Vehicular Ad-Hoc Networks of V2I Communication. *Procedia Comput. Sci.* **2015**, *54*, 215–223. [CrossRef]
44. Perrig, A.; Stankovic, J.; Wagner, D. Security in wireless sensor networks. *Commun. ACM* **2004**, *47*, 53–57. [CrossRef]
45. Malla, A.M.; Sahu, R.K. Security Attacks with an Effective Solution for Dos Attacks in VANET. *Int. J. Comput. Appl.* **2013**, *66*, 45–49.
46. Song, L.; Han, Q.; Liu, J. Investigate Key Management and Authentication Models in VANETs. In Proceedings of the 2011 International Conference on Electronics, Communications and Control (ICECC), Ningbo, China, 9–11 September 2011; pp. 1516–1519. [CrossRef]

47. Memon, I.; Arain, Q.A.; Memon, M.H.; Mangi, F.A.; Akhtar, R. Search me if you can: Multiple mix zones with location privacy protection for mapping services. *Int. J. Commun. Syst.* **2017**, *30*, e3312. [CrossRef]
48. Memon, I.; Ali, Q.; Zubedi, A.; Mangi, F.A. DPMM: Dynamic Pseudonym-based Multiple Mix-zones Generation for Mobile Traveler. *Multimed. Tools Appl.* **2017**, *76*, 24359–24388. [CrossRef]
49. Arain, Q.A.; Uqaili, M.A.; Deng, Z.; Memon, I.; Jiao, J.; Shaikh, M.A.; Zubedi, A.; Ashraf, A.; Arain, U.A. Clustering Based Energy Efficient and Communication Protocol for Multiple Mix-zones over Road Networks. *Wirel. Pers. Commun.* **2018**, *95*, 411–428. [CrossRef]
50. Memon, I.; Arain, Q.A. Dynamic Path Privacy Protection Framework for Continuous Query Service over Road Networks. *World Wide Web* **2017**, *20*, 639–672. [CrossRef]
51. Memon, I. A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks. *Wirel. Pers. Commun.* **2015**, *85*, 1167–1191. [CrossRef]
52. Domenic, M.K.; Wang, Y.; Zhang, F.; Memon, I.; Gustav, Y.H. Preserving Users' Privacy for Continuous Query Services in Road Networks. In Proceedings of the 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering, Xi'an, China, 23–24 November 2013; Volume 1, pp. 352–355. [CrossRef]
53. Gustav, Y.H.; Wang, Y.; Domenic, M.K.; Zhang, F.; Memon, I. Velocity Similarity Anonymization for Continuous Query Location Based Services. In Proceedings of the 2013 International Conference on Computational Problem-Solving (ICCP), Jiuzhai, China, 26–28 October 2013; pp. 433–436. [CrossRef]
54. Dahiya, A.; Sharma, V. A Survey on Securing User Authentication Vehicular Ad Hoc Networks. *Int. J. Inf. Secur.* **2001**, *1*, 164–171.
55. Raiya, R.; Gandhi, S. Survey of Various Security Techniques in VANET. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2014**, *4*, 431–433.
56. Caballero-Gil, P. Security Issues in Vehicular Ad Hoc Networks. In *Book Mobile Ad-Hoc Networks: Applications*; Wang, X., Ed.; IntechOpen: London, UK, 2011; pp. 67–88.
57. Jayalakshmi, N.; Rajadurai, R.; Indumathi, K. Vehicular Network: Properties, Structure, Challenges, Attacks, Solution for Improving Scalability and Security. *Int. J. Sci. Eng. Res.* **2013**, *4*, 152–159.
58. Blum, J.; Eskandarian, A. The Threat of Intelligent Collisions. *IT Prof.* **2004**, *6*, 24–29. [CrossRef]
59. Schuba, C.L.; Krsul, I.V.; Kuhn, M.G.; Spafford, E.H.; Sundaram, A.; Zamboni, D. Analysis of a denial of service attack on TCP. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 4–7 May 1997; pp. 208–223. [CrossRef]
60. Kuzmanovic, A.; Knightly, E.W. Low-rate TCP-targeted denial of service attacks and counter strategies. *IEEE ACM Trans. Netw.* **2006**, *14*, 683–696. [CrossRef]
61. Romero-Zurita, N.; Ghogho, M.; McLernon, D. Outage probability based power distribution between data and artificial noise for physical layer security. *IEEE Signal Process. Lett.* **2012**, *19*, 71–74. [CrossRef]
62. Jung, C.D.; Sur, C.; Park, Y.; Rhee, K.H. A Robust Conditional Privacy-Preserving Authentication Protocol in VANET. In *Book Security and Privacy in Mobile Information and Communication Systems. MobiSec 2009*; Schmidt, A.U., Lian, S., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Berlin, Germany, 2009; Volume 17, pp. 35–45.
63. Zhou, W.; Marshall, A.; Gu, Q. A Novel Classification Scheme for 802.11 WLAN Active Attacking Traffic Patterns. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2006), Las Vegas, NV, USA, 3–6 April 2006; Volume 2, pp. 623–628. [CrossRef]
64. Wang, H.; Yin, Q.; Xia, X. Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks. *IEEE Trans. Signal Process.* **2012**, *60*, 3532–3545. [CrossRef]
65. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
66. CA-1995.01: IP spoofing Attacks and Hijacked Terminal Connections. In *Book 1995 CERT Advisories*; Carnegie Mellon University: Pittsburgh, PA, USA, 2017; pp. 2–14. Available online: https://resources.sei.cmu.edu/asset_files/WhitePaper/1995_019_001_496168.pdf (accessed on 31 August 2018).
67. Elliott, C. Quantum cryptography. *IEEE Secur. Priv.* **2004**, *2*, 57–61. [CrossRef]
68. Chang, R.K.C. Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Commun. Mag.* **2002**, *40*, 42–51. [CrossRef]

69. Aslam, B.; Zou, C.C. Distributed certificate and application architecture for VANETs. In Proceedings of the MILCOM 2009—2009 IEEE Military Communications Conference, Boston, MA, USA, 18–21 October 2009; pp. 1–7. [CrossRef]
70. He, X.; Khisti, A.; Yener, A. MIMO broadcast channel with arbitrarily varying eavesdropper channel: Secrecy degrees of freedom. In Proceedings of the 2011 IEEE Global Telecommunications Conference—GLOBECOM 2011, Kathmandu, Nepal, 5–9 December 2011; pp. 1–5. [CrossRef]
71. Wei, Y.; Zengy, K.; Mohapatra, P. Adaptive Wireless channel probing for shared key generation. In Proceedings of the IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 2165–2173. [CrossRef]
72. Araujo, A.; Blesa, J.; Romero, E.; Nieto-Taladriz, O. Artificial noise scheme to ensure secure communications in CWSN. In Proceedings of the 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 27–31 August 2012; pp. 1023–1027. [CrossRef]
73. Park, J.; Kasera, S. Securing Ad Hoc wireless networks against data injection attacks using firewalls. In Proceedings of the IEEE Wireless Communications and Networking Conference, Kowloon, China, 11–15 March 2007; pp. 2843–2848. [CrossRef]
74. Stolyarova, E.S.; Shiryaev, D.M.; Vladyko, A.G.; Buinevich, M.V. VANET/ITS Cybersecurity Threats: Analysis, Categorization and Forecasting. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 29 January–1 February 2018; pp. 136–141. [CrossRef]
75. Sumra, I.A.; Ahmad, I.; Hasbullah, H.; Manan, J. Classes of attacks in VANET. In Proceedings of the 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 24–26 April 2011; pp. 1–5. [CrossRef]
76. Sumra, I.A.; Hasbullah, H.B.; Manan, J.; Ahmad, I.; Alghazzawi, D.M. Classification of Attacks in Vehicular Ad hoc Network (VANET). *Inf. Int. Interdiscip. J.* **2013**, *16*, 2995–3004.
77. Nema, M.; Stalin, S.; Lokhande, V. Analysis of Attacks and Challenges in VANET. *Int. J. Emerg. Technol. Adv. Eng.* **2014**, *4*, 831–835.
78. Mostovich, D.; Fabrikantov, P.; Vladyko, A.; Buinevich, M. High-Level Vulnerabilities of Software-Defined Networking in the Context of Telecommunication Network Evolution. In Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Russia, 29 January–1 February 2017; pp. 184–186. [CrossRef]
79. Chiasson, G.; Hays, D.; Nalinakshan, H.; Ranganna, S. Are Wi-Fi and 4G LTE on a collision course. *PwC Commun. Rev.* **2015**. Available online: https://www.pwc.com/id/en/publications/assets/ticepublications/pwc-communications-review-wi-fi-4g-lte_final.pdf (accessed on 2 January 2019).
80. Said, S.B.H.; Guillouard, K.; Bonnin, J.M. A Comparative Study on Security implementation in EPS/LTE and WLAN/802.11. In *Book Wireless Networks and Security*; Khan, S., Pathan, A.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 457–489.
81. Volkov, A.; Khakimov, A.; Muthanna, A.; Kirichek, R.; Vladyko, A.; Koucheryavy, A. Interaction of the IoT Traffic Generated by a Smart City Segment with SDN Core Network. *Lect. Notes Comput. Sci.* **2017**, *10372*, 115–126. [CrossRef]
82. Di Maio, A.; Palattella, M.R.; Soua, R.; Lamorte, L.; Vilajosana, X.; Alonso-Zarate, J.; Engel, T. Enabling SDN in VANETs: What is the Impact on Security? *Sensors* **2016**, *16*, 2077. [CrossRef]
83. The OWASP Foundation. Available online: https://www.owasp.org (accessed on 31 August 2018).
84. Shila, D.M.; Cao, X.; Cheng, Y.; Yang, Z.; Zhou, Y.; Chen, J. Ghost-in-the-Wireless: Energy Depletion Attack on ZigBee. *arXiv* **2014**, arXiv:1410.1613.
85. Kirichek, R.; Kulik, V.; Koucheryavy, A. False Clouds for Internet of Things and Methods of Protection. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, South Korea, 31 January–3 February 2016; pp. 201–205. [CrossRef]
86. Buinevich, M.; Izrailov, K.; Vladyko, A. The Life Cycle of Vulnerabilities in the Representations of Software for Telecommunication Devices. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31 January–3 February 2016; pp. 430–435. [CrossRef]
87. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A. Security in Software Defined Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2317–2346. [CrossRef]

88. Scott-Hayward, S.; Natarajan, S.; Sezer, S. A Survey of Security in Software Defined Networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 623–654. [CrossRef]
89. Ahmed, U.; Raza, I.; Hussain, S.A.; Ali, A.; Iqbal, M.; Wang, X. Modelling Cyber Security for Software-Defined Networks Those Grow Strong when Exposed to Threats. *J. Reliab. Intell. Environ.* **2015**, *1*, 123–146. [CrossRef]
90. Yan, Z.; Zhang, P.; Vasilakos, A.V. A Security and Trust Framework for Virtualized Networks and Software-Defined Networking. *Secur. Commun. Netw.* **2016**, *9*, 3059–3069. [CrossRef]
91. Dotcenko, S.; Vladyko, A.; Letenko, I. A Fuzzy Logic-Based Information Security Management for Software-Defined Networks. In Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 16–19 February 2014; pp. 167–171. [CrossRef]
92. Weber, R.H. Internet of Things—New Security and Privacy Challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
93. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the Internet of Things: A Review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 23–25 March 2012; pp. 648–651.
94. Roman, R.; Najera, P.; Lopez, J. Securing the Internet of Things. *Computer* **2011**, *44*, 51–58. [CrossRef]
95. Zhou, L.; Chao, H.C. Multimedia Traffic Security Architecture for the Internet of Things. *IEEE Netw.* **2011**, *25*, 35–40. [CrossRef]
96. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
97. Saaty, T.L. How to make a decision: The analytic hierarchy process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [CrossRef]
98. Saaty, T.L. Decision-making with the AHP: Why is the principal eigenvector necessary. *Eur. J. Oper. Res.* **2003**, *145*, 85–91. [CrossRef]
99. Buinevich, M.; Fabrikantov, P.; Stolyarova, E.; Izrailov, K.; Vladyko, A. Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast. In Proceedings of the 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), Moscow, Russia, 20–22 September 2017.
100. Kazmi, A.; Khan, M.A.; Akram, M.U. DeVANET: Decentralized Software-Defined VANET Architecture. In Proceedings of the IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 4–8 April 2016; pp. 42–47. [CrossRef]
101. European Commission. *European Strategy on Cooperative Intelligent Transport Systems, a Milestone Initiative Towards Cooperative, Connected and Automated Mobility*; Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS; European Commission: Brussels, Belgium, 2016.
102. Bouk, S.H.; Ahmed, S.H.; Hussain, R.; Eun, Y. Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS. *IEEE Access* **2018**, *6*, 60570–60585. [CrossRef]